POLYCOM®

▶ Polycom RMX 1500/2000/4000

Release Notes

for Maximum Security Environments

This software meets the latest U.S. Department of Defense network requirements for listing on the Defense Switched Network (DSN) Approved Products List (APL), as maintained by the Joint Interoperability Test Command (JITC).

This document provides the latest information for security-conscious users running version 7.5.0.J software.

Table of Contents

New Hardware - RMX 1500

A new MCU has been added to the RMX family of MCUs.
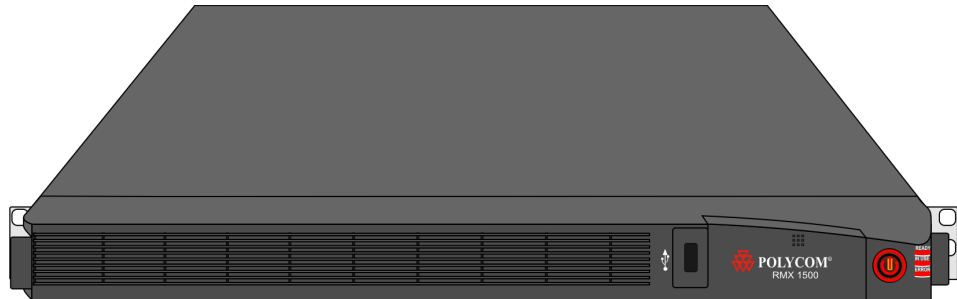
It has the key features of the RMX 2000 and RMX 4000 with the following additions/changes:

Table 1   *RMX 1500 Additions and Changes*

	Feature Name	Description
1	New card	New cards and modified components have been added to the Hardware.
2	System Capacity	One MPMx media card is installed on the system and this is reflected in the: • Network Services • Video/Voice Port Configuration • Resource Report
3	RMX Type Indication	RMX Banner and Welcome heading display the RMX Type accordingly.
4	Hardware Monitor	New and dedicated slots. New card properties.

For detailed description of the new MCU attributes, see "*Detailed Description - RMX 1500"* on page **31**.

New Hardware - MPMx Media Card

The new *MPMx* card (*Media Processing Module*) when installed in *RMX* running *Version 7.5.0.J* offers:

*   Increased resource capacity
*   New Symmetric HD Video resolutions 720p60 & HD1080p30 fps
*   Support for H.264 High Profile

Two types of *MPMx* cards are available:

*   *MPMx - S* (Single)
*   *MPMx - D* (Double)

The following table lists the changes in Version 7.5.0.J to support the new MPMx card:.

Table 2   *MPMx Card - Additions to Version 7.5.0.J*

	Category	Feature Name	Description
1	General	Card Configuration Mode	A new *Card Configuration Mode - MPMx* has been added to support the new media card.
2	General	Hardware Monitor	The status and properties of the *MPMx* card can be viewed and monitored in the *Hardware Monitor* list pane.
3	General	Video/Voice Port Configuration	The *Resource* slider(s) in the *Video/ Voice Port Configuration* dialog box reflect the *MPMx* card capacities.
4	General	Resource Report	The resource report reflects the *MPMx* card capacities.
5	General	Port Gauges	The *Video/Voice Port* gauges reflect the *MPMx* card capacities.

Version 7.5.0.J - New Security Features

The following table lists the new features in Version 7.5.0.J.

Table 3   *New Features List*

	Category	Feature Name	Description
1	General	Direct Connection to Polycom RMX™ Serial Gateway S4GW	To meet UC APL Public Key Infrastructure (PKI) requirements, the Serial Gateway S4GW is connected directly to the RMX and not to the H.323 network. A new System Flag, V35_ULTRA _SECURED_SUPPORT has been added to support this feature.
2	Security	PKI	PKI (Public Key Infrastructure) is a set of tools and policies deployed to enhance the security of data communications between networking entities.
3		Machine Account	User names of *Application-users* such as CMA and DMA can be associated with servers (machines) to ensure that all users are subject to the same account and password policies.
4		Active Directory	This version introduces direct interaction between the RMX and Microsoft Active Directory for Authentication and Authorization of Management Network users.
5		Multiple Networks	Media, signaling and Management networks can be physically separated on the RMX system to provide enhanced security.
6		Antivirus	McAfee® Antivirus application can be enabled and scheduled to scan for viruses.
7		Information Collector - (NIDS)	Enables the administrator to view the Network Intrusion Detection System (NIDS) log that includes all unpermitted access attempts blocked by the fire wall. Unpermitted access includes: access to ports which are not opened in the RMX; invalid access to open ports.

Version 7.5.0.J - Changes to Existing Security Features

The following table lists the changes to existing features in Version 7.5.0.J.

Table 4   *Feature Changes List*

	Category	Feature Name	Description
1	General	V.35 Gateway Tab in IP Network Service Dialog Box	The IP Network Service dialog box has a new tab, V.35 Gateway enabling the administrator to add the gateway to a new or existing IP Network Service.
2		Additional Log Events	Firewall denials and errors pertaining to the MCMS will be logged by the Logger utility and Auditor:
3	Hardware	MPM+ or MPMx cards	*Version 7.5.0.J* requires MPM+ or MPMx cards to be installed in the RMX.
4	Security	ULTRA_SECURE _MODE Flag	Ultra Secure Mode, is enabled by manually adding the ULTRA_SECURE_MODE flag to the System Configuration and setting its value to YES.
5		Login and Main Page Banner Name Changes	The administrator can choose one of four alternative login banners to be displayed. The four alternative banners cannot be modified. A Custom banner (default) can also be defined. The Main Page Banner is blank and can be defined.
6		User Management	*User Name* is now case sensitive
7		Strong Passwords	Password management now includes definition of *Maximum Repeating Characters* for Conference and Chairperson Passwords. **Note:** *Chairperson* users are not supported in *Ultra Secure Mode*.
8		USB Restore to Default	The USB port of an RMX in Ultra Secure Mode can be used to: • Restore the RMX to Factory Security Defaults mode (https → http). • Perform a Comprehensive Restore to Factory Defaults

Version 7.5.0.J - New Features

The following table lists the new features in Version 7.5.0.J

Table 5   *New Features List*

	Category	Feature Name	Card Configuration Mode	Description
1	Audio	Audio Clarity	MPM+ MPMx	Audio Clarity improves received audio from participants connected via ISDN/PSTN using the following low bandwidth (4kHz) audio algorithms: G.729a and G.711.
2		Packet Loss Concealment (PLC)	MPM+ MPMx	Packet Loss Concealment (PLC) for Siren audio algorithms improves received audio when packet loss occurs in the network. The following audio algorithms are supported: • Siren 7 (mono) • Siren 14 (mono/stereo) • Siren 22 (mono/stereo)
3		Siren 22 Audio Algorithm	MPM+ MPMx	Polycom's proprietary Siren 22 Audio Algorithm is supported for participants connecting with Polycom endpoints. Both Mono and Stereo are supported.
4		Siren 14 - Stereo	MPM+ MPMx	Added support for Siren 14 Stereo. Siren 14 Stereo is supported at line rates between 256Kbps and 4096Kbps. Siren 14 Stereo is supported by HDX endpoints and VSX endpoint (with the exception of VSX 500).
5		G.719 Audio Algorithm	MPM+ MPMx	G.719 audio algorithm is supported for participants connecting with Polycom endpoints. Both Mono and Stereo are supported.
6		G. 728	MPM+	Industry standard *G.728* audio algorithm is supported for participants connecting with legacy or low bandwidth endpoints.
7	Conference	Permanent Conference	MPM+ MPMx	A *Permanent Conference* is an ongoing conference with no pre-determined *End Time* continuing until it is terminated by an administrator, operator or chairperson. **Note:** *Chairperson* users are not supported in *Ultra Secure Mode*.
8		Video Preview	MPM+ MPMx	*RMX* users can preview the video sent from the participant to the conference (*MCU*) and the video sent from the conference to the participant. It enables the *RMX* users to monitor the quality of the video sent and received by the participant and identify possible quality degradation.

Table 5 *New Features List (Continued)*

	Category	Feature Name	Card Configuration Mode	Description
9	Conference (cont.)	Personal Conference Manager (PCM)	MPM+	The *Personal Conference Manager* (*PCM*) interface enables the conference chairperson to control various conference features using his/her endpoint's remote control device. **Note:** *Chairperson* users are not supported in *Ultra Secure Mode*.
10		Message Overlay	MPM+ MPMx	Using the *Message Overlay* option, a message can be sent to all the participants in a conference and displayed on their endpoint screens.
11		Content Broadcast Control	MPM+ MPMx	*Content Broadcast Control* prevents the accidental interruption or termination of *H.239 Content* that is being shared in a conference by giving *Content Token* ownership to a specific endpoint via the *RMX Web Client.*
12		Copy, Cut, Paste Participant	MPM+ MPMx	The RMX user can Copy, Cut and Paste participants between different conferences running on the RMX.When used via the RMX Manager, the user can Copy, Cut and Paste participants between conferences running on different RMXs.
13		Copy, Paste Conference	MPM+ MPMx	The RMX user can Copy and Paste conferences on the same RMX and, when used via the RMX Manager, between different RMXs.
14		Gathering Slide	MPM+ MPMx	Once connected to the conference, a special slide, the Gathering Slide, is displayed to connected participants until the conference starts. The Gathering Slide displays live video along with information taken from the meeting invitation.

Table 5   *New Features List (Continued)*

	Category	Feature Name	Card Configuration Mode	Description
15	General (cont.)	Resolution Configuration	MPM+ MPMx	The *Resolution Configuration* dialog box enables *RMX* administrators to override the predefined video resolution matrix.
16		High Resolution Slide Enhancements	MPM+ MPMx	*Conference* and *Entry Queue IVR Services* now support customized *High Resolution Slides* in addition to the low and high resolution slides included in the default slide set.
17		Multiple Recording Links	MPM+ MPMx	The *Multiple Recording Links* feature enables *Conference Recording Links*, defined on the *RMX* to be associated with *Virtual Recording Rooms* (*VRR*), created and saved on the *Polycom® RSS™ 4000 Version 6.0 Recording And Streaming Server* (*RSS*). **Note:** *Recording Links* are not supported in *Ultra Secure Mode*.
18		Auto Redial when Endpoint Drops	MPM+ MPMx	The *Auto Redialing* option instructs the *RMX* to automatically redial *IP* and *SIP* participants that have been abnormally disconnected from the conference.
19		Multi-RMX Manager Export/Import RMX Configuration	MPM+ MPMx	The RMX Manager configuration that includes the MCU list and the multilingual selection can be saved to any workstation/PC on the network and imported to any Multi-RMX Manager installed in the network.
20		Automatic Password Generation	MPM+, MPMx	The RMX can be configured to automatically generate conference and chairperson passwords when the Conference Password and Chairperson Password fields are left blank. **Note:** *Chairperson* users are not supported in *Ultra Secure Mode*.
21		RMX as IVR Service Provider to DMA	MPM+, MPMx	In an environment that includes a DMA, the RMX Entry Queue can be configured to be used only as provider of IVR Services to SIP endpoints that connect to the DMA and retrieve the Conference ID entered using DTMF codes.

Table 5   *New Features List (Continued)*

	Category	**Feature Name**	**Card Configura-tion Mode**	**Description**
22	Video	Auto Brightness	MPM+ MPMx	Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.
23		H.264 High Profile	MPMx	The *H.264 High Profile* improves video quality and can reduce bandwidth requirements for video conferencing transmissions by up to 50%.
24		New Symmetric HD Resolutions	MPMx	New Symmetric *HD* video resolutions *HD 1080p30* and *HD 720p60* have been added.
25		Additional Call Rates	As per table	New *Call Rates* have been added.
26		People+Content	MPM+ MPMx	*Polycom's* proprietary *People+Content*, which is the equivalent of *H.239* is supported in addition to *H.239*.

Version 7.5.0.J - Changes to Existing Features

The following table lists the changes to existing features in Version 7.5.0.J.

Table 6   *Changes to Existing Features*

	Category	Feature Name	Description
1	Audio	Audio Only Message	In this version, the administrator can enable an audio message that informs the participant of the lack of *Video Resources* in the *RMX* and that he/she is being connected as *Audio Only*.
2		*Audio Settings* tab in *New Profile* dialog box	A new tab *Audio Settings* has been added to the *New Profile* dialog box. It contains settings for: • Echo Suppression • Keyboard Noise Suppression • Audio Clarity
3	CMA/DMA	RMX Resource Management by CMA and DMA	In this version, following a request by the CMA and DMA, the RMX will send updates on resource usage to both CMA and DMA, with each application updating its own resource usage for the RMX. This provides better management of the RMX resources by CMA and DMA.

Table 6   *Changes to Existing Features (Continued)*

	Category	Feature Name	Description
4	General	IVR Service	The DTMF Codes of the Roll Call actions defined in the default IVR Services shipped with new RMX systems were changed as follows: • Enable Roll Call: old: *32 new: *42 • Disable Roll Call: old: #32 new: #42 • Roll Call Review Names: old: *33 new: *43 • Roll Call Stop Review: old: #33 new: #43
5		IVR Service	The DTMF Codes of the Recording actions defined in the default IVR Services shipped with new RMX systems were changed as follows: • Start/Resume Recording: old: *73 new: *3 • Stop Recording: old: *74 new: *2 • Pause Recording: old: *75 new: *1 **Note:** *Recording* is not supported in *Ultra Secure Mode*.
6		Multilingual Support	Site names can now be displayed in Kazakh fonts.
7		System Configuration Flag	The flag: **ITP_CROPPING** was added to determine the automatic cropping performed by the system when adjusting the display aspect ratio from 9:16 to 3:4 and vice versa in Telepresence (ITP) conferences. The following values can be defined: • **ITP** (default) - When a Telepresence (ITP) conference is detected, the image will not be cropped on the sides, but either black strips will be added to the top and bottom (when adjusting the aspect ratio from 9:16 to 3:4) or strips will be cropped from the top and the bottom at a ratio of 84%:16% (for 3:4 to 9:16 ratio adjustment). This setting is compatible with system behavior in previous versions. • **CP** - cropping is performed equally from top and bottom or from the sides (depending on the required ratio adjustment), as done in non-telepresence conferences (CP conferences). • **MIXED** - cropping is performed equally from the sides of the picture (as in CP mode) and 84%/16% from top and bottom as in ITP mode, depending on the required ratio adjustment.

Table 6   Changes to Existing Features (Continued)

	Category	Feature Name	Description
8	General (cont.)	DTMF Forwarding Suppression	Forwarding of the DTMF codes from one conference to another over an ISDN cascading link can be limited to basic operations while suppressing all other operations once the connection between the cascaded conferences is established. **Note:** *ISDN Cascading* is not supported in *Ultra Secure Mode*.
9		Integration with Polycom CMA™ Global Address Book	The definition of the CMA IP address for the EXTERNAL_CONTENT_IP flag has changed and in this version only the IP address is entered (without http://). For more details, see RMX 1500/2000/4000 Administrator's Guide, "*Integrating the Polycom CMA™ Address Book with the RMX"* on page **6-23**.
10		Resolution Sliders	The System Flags that were introduced in version 7.0.1 were incorporated into the Resolution Configuration dialog box designed to enable the administrator to modify the minimum bit rate thresholds of the H.264 Base Profile and High Profile for the various pre-configured resolution matrices so video quality is maintained when endpoints supporting H.264 High Profile and Base Profile connect to the same conference.
11		System Configuration Flag	The flag **CPU_TCP_KEEP_ALIVE_TIME_ SECONDS** was added to the system configuration. This flag indicates when to send the first KeepAlive indication to check the TCP connection. Default value: **7200** second (60 minutes) Range: 600-18000 seconds When there are NAT problems, this default may be too long and the TCP connection is lost. In such a case, the default value should be changed to 3600 seconds (30 minutes) or less.
12		System Configuration Flag	The flag **CPU_TCP_KEEP_INTERVAL_ SECONDS** was added to the system configuration. This flag indicates the interval in seconds between the KeepAlive requests. Default value: **75** second Range: 10-720 seconds.

Table 6   *Changes to Existing Features (Continued)*

	Category	Feature Name	Description
13	General (cont.)	System Configuration Flag	The flag **ITP_CERTIFICATION** was added to the system configuration. When set to **NO** (default), disables the telepresence features in the Conference Profile. Set the flag to **YES** to enable the telepresence features in the Conference Profile (provided that the appropriate License is installed).
14		System Configuration Flag	The **H323_RAS_IPV6** was added tot the system configuration. When IPv4 & IPv6 addressing is selected, RAS (Registration, Admission, and Status) messages are sent in both IPv4 and IPv6 format. If the gatekeeper cannot operate in IPv6 addressing mode, registration fails and endpoints cannot connect using the RMX prefix. In such cases this System Flag should be set to **NO**. Default: **YES**
15	Video	Telepresence Mode	Control and monitoring of *Immersive Telepresence* (*ITP*) features have been enhanced with: • Automatic detection of *ITP* sites. • Retrieval of *Telepresence Layout Mode.* • Control of *Cropping* and *Striping* options. • Enhanced *Layout* control.
16		Limiting Maximum Resolution	The *Maximum Resolution* settings of the *Resolution Configuration* dialog box can be overridden by new fields that have been included in the *New Profile* and *New Participant* dialog boxes.
17		Auto Layout Changes	Two additional layouts are activated in Auto Layout Mode when there are: • 11 connected participants • 12 or more connected participants
18		Auto Brightness	*Auto Brightness* detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.
19		Video Switching Resolutions	In addition to *H.264 720p30*, the following *Video Switching* resolutions have been added for *MPM+* and *MPMx* cards only: • H.264 1080p30 • H.264 720p60 • H.264 SD 30

Version 7.5.0.J - Interoperability Tables

Devices

The following table lists the devices with which Version 7.5.0.J was tested.

Table 7   *Version 7.5.0.J Device Interoperability Table*

Device	Version
Gatekeepers/Proxies	
Polycom CMA	5.4.0, 5.2.0.J
Polycom DMA	*DMA 2.3, DMA 2.1.0.J*
Polycom PathNavigator	7.0.14
Polycom SE200	3.00.07.ER001
Cisco gatekeeper	12.3
Radvision ECS gatekeeper	3.5.2.5
Iptel proxy	1.0.2
Broadsoft proxy	BroadWorks release 14 sp9
Recorder	
Polycom RSS 2000	4.0.0.001 360
Polycom RSS 4000	6.4.0.0-26517
MCUs, Call Managers Network Devices and Add ins	
Polycom MGC 25/50/100 and MGC+50/100	8.0.2 and 9.0.3
RMX 1000	2.1.2
Polycom DMA 7000	2.3, *2.1.0.J*
Polycom RMX™ Serial Gateway S4GW	*GWUpgradePack_Polycom_5_7_2_7_27*
Avaya CM	5.2
Avaya ACM	2.1.016.4-18111, 943
Avaya IP Softphone	R6.0 SP1
Cisco Call Manager	4.1, 8.0.5
Tandberg MCU	D3.11
Tandberg MPS	J3.3
Polycom VBP 5300LF-S25	9.1.5.3
Polycom VBP - E	9.1.5.3
Polycom Conferencing Add in for Microsoft Outlook	1.0.2

Table 7   *Version 7.5.0.J Device Interoperability Table (Continued)*

Device	Version
Endpoints	
Polycom HDX Family	3.0.0, 3.0.1, 2.7.0_J
Polycom Telepresence (ITP) Systems	2.6, 2.7
Polycom VSX and V-Series Family	9.0.6.1
Polycom Viewstation Family	7.5.4
Polycom CMA Desktop	5.1.0.0060
Polycom QDX6000	4.0.1
Polycom VVX1500	3.3.1
SoundPointIP 650	3.2.2
Polycom PVX	8.0.16
Polycom VS Family	7.5.4
Polycom VS FX Family (EX, FX, 4000)	6.0.5
Polycom iPower 9000	6.2.1208
Soundstation IP3000	2.8
Aethra X3	12.1.19
Aethra X7	12.1.7
Aethra VegaStar Gold	6.0.49
Avaya IP Softphone	R6 6.01.48
Avaya 1XC Communicator	R1.020-SP2-1696
LifeSize 200	4.7.11.4
LifeSize Room and Express	4.7.11.4
VVX1500	3.3.1
DST B5	2.0
DST K60	2.0.1
DST K80	4.0
Sony PCS -XG80	2.11
Sony PCS -1	3.42
Sony PCS -G family	2.72
Sony PCS -TL50	2.42
Tandberg 150 MXP	L6.0.2
Tandberg MXP F-Series Family	F9.0.1
Tandberg 6000 B	B10.3
Tandberg Classic E Family	E5.3

Table 7   *Version 7.5.0.J Device Interoperability Table (Continued)*

Device	Version
Tandberg EX90	3.1.3
Tandberg C Family	3.1.3
Tandberg E20	2.2.1
RadVision E.P SCOPIA XT1000	2.0.18
RadVision SCOPIA E.P	RV-VC240-2
Microsoft OC client R2	R2 3.5.6907.196
Microsoft Lync client	v4.0.7577.0
Vidyo Desktop client	2.0.4

Polycom RMX and Avaya Interoperability

For questions and support on the Polycom - Avaya integrated solution, contact your Avaya Authorized Service Provider.

The Polycom RMX 2000/4000 series of MCUs running software version 7.0.1.16 register to current generally available versions of Avaya Aura Session Manager R6.0 to provide multipoint video calls.

Polycom RMX 4000, RMX 2000 and RMX 1500 can call and receive calls with current generally available versions of Avaya one-X Communicator H.323 video soft clients (R5.2) on Communication Manager R5.2.1 and R6.0.

RMX Web Client

The following table lists the environments (Web Browsers and Operating Systems) with which the *RMX Web Client* was tested.

Table 8   *Environment Interoperability Table*

Web Browser	Operating System
Internet Explorer 6	Windows XP™
Internet Explorer 7	Windows XP™
	Windows Vista™
	Windows 7
Internet Explorer 8	Windows 7

Windows 7™ Security Settings

If *Windows 7* is installed on the workstation, *Protected Mode* must be disabled before downloading the Version 7.0 software to the workstation.

To disable Protected Mode:

1   In the *Internet Options* dialog box, click the **Security** tab.

     The **Security** tab is displayed.
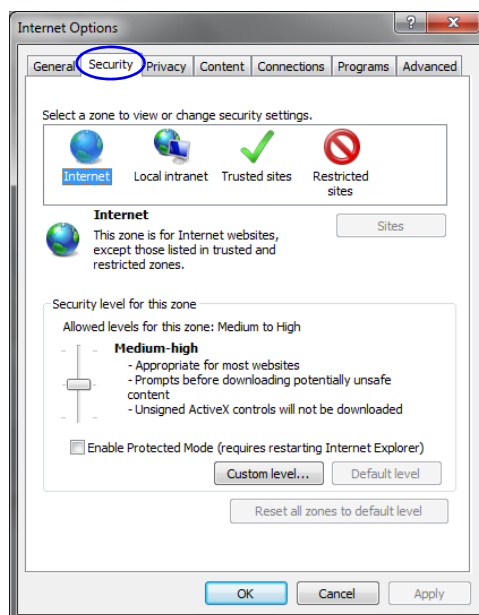
2   Clear the *Enable Protected Mode* check box for each of the following tabs:

— *Internet*

— *Local intranet*

— *Trusted sites*
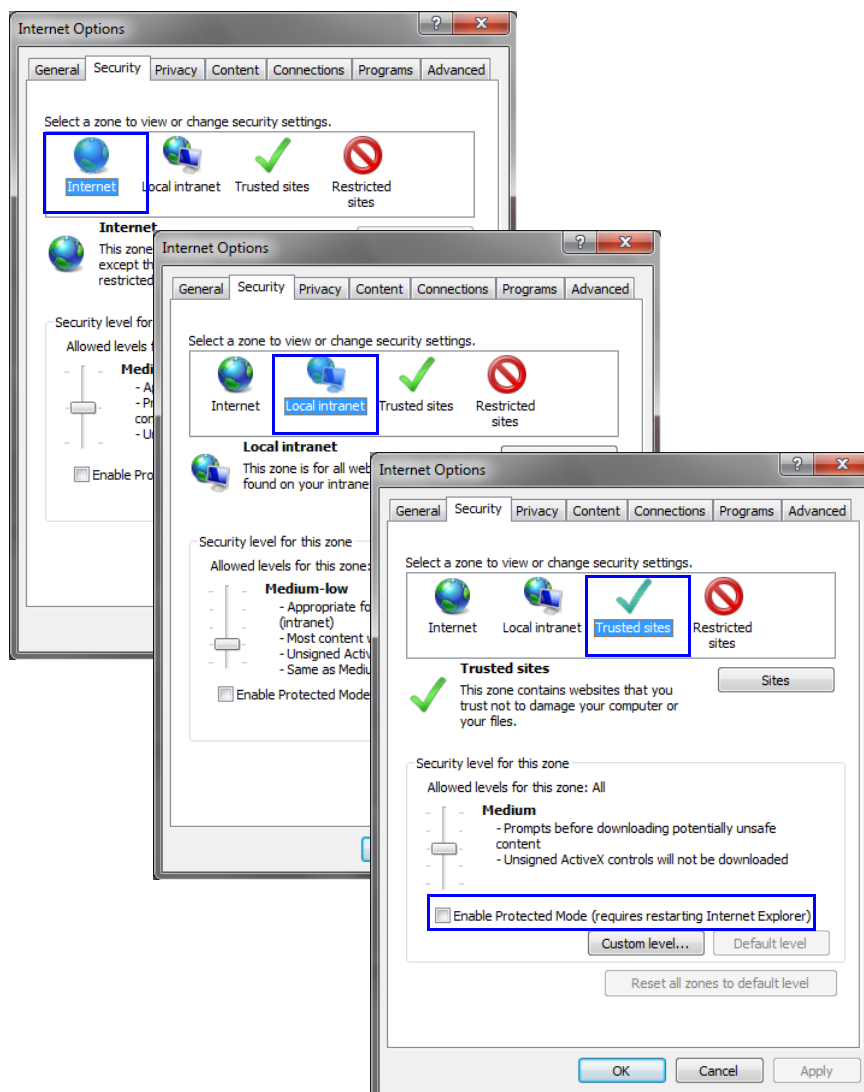
3   After successful connection to *RMX*, the *Enable Protected Mode* check boxes can be selected to enable *Protected Mode* for the following tabs:

— *Internet*

— *Local intranet*

17

Internet Explorer 8 Configuration

When using *Internet Explorer 8* to run the *RMX Web Client* or *RMX Manager* applications, it is important to configure the browser according to the following procedure.

To configure Internet Explorer 8:

1 Close **all** browsers running on the workstation.

2 Use the *Windows Task Manager* to verify that no *iexplore.exe* processes are running on the workstation. If any processes are found, use the **End Task** button to end them.

3 Open *Internet Explorer* but do **not** connect to the *RMX*.

4 In the *Internet Explorer* menu bar select **Tools >> Internet Options**.

The *Internet Options* dialog box is displayed with *General* tab open.
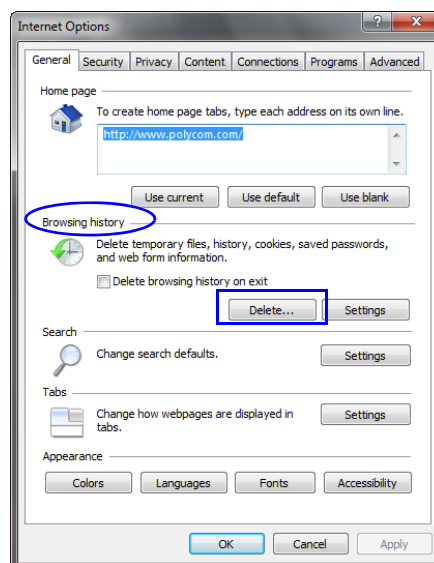
5 In the *Browsing history* section, click the **Delete** button.

The *Delete Browsing History* dialog box is displayed.
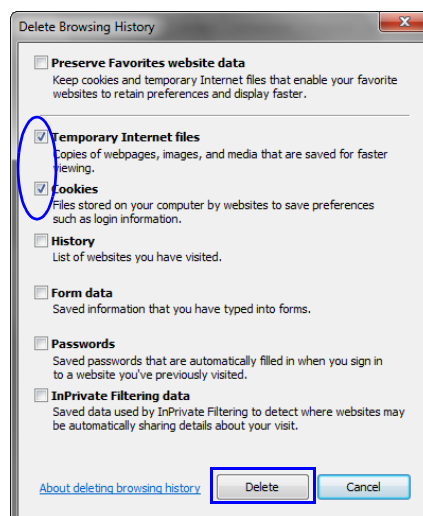
6 Select the **Temporary Internet** files and **Cookies** check boxes.

7 Click the **Delete** button.

8 The *Delete Browsing History* dialog box closes and the files are deleted.

9 In the *Internet Options* dialog box, click the **Settings** button.

The *Temporary Internet Files and History Settings* dialog box is displayed.
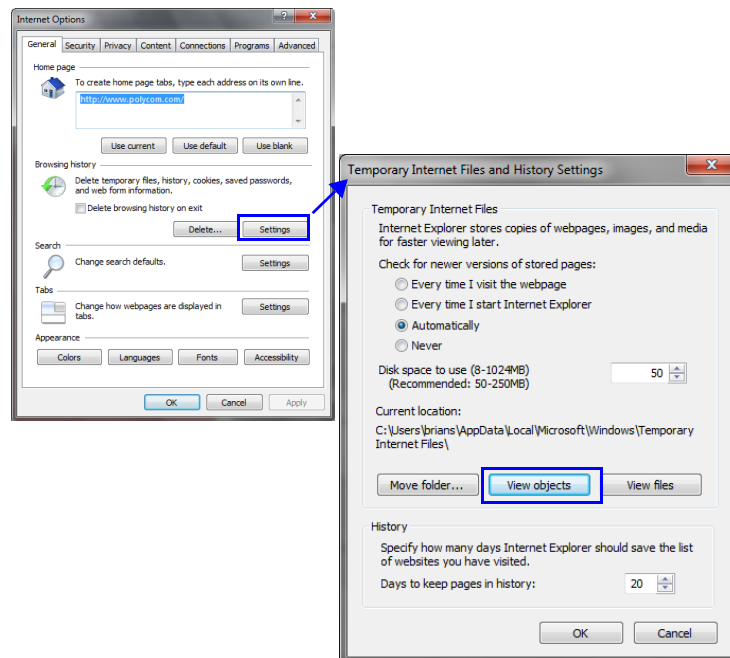
10 Click the **View objects** button.

The *Downloaded Program Files* folder containing the installed *Program Files* is displayed.
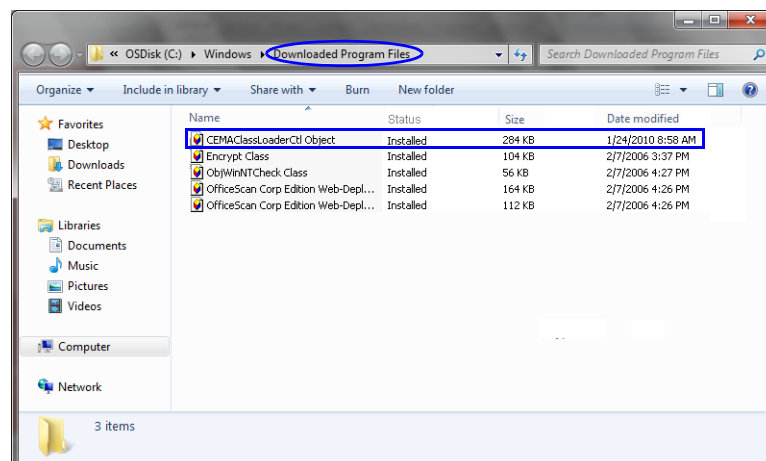
11 Select the *CEMAClassLoaderCntl Object* file

12 Press the **Delete** key on the workstation.

13 Close the *Downloaded Program Files* folder and the *Temporary Internet Files and History Settings* dialog box.

14 In the *Internet Options* dialog box, click the **OK** button to save the changes and close the dialog box.

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services will help customers successfully design, deploy, optimize and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Unsupported Features

When the **ULTRA_SECURE_MODE** flag is set to **YES,** *Version 7.5.0.J* does not include support for:

- Connection to Alternate Management Network via LAN3 port

- SUPPORT user
- Auditor user
- Chairperson user
- Connections to External Databases
- IP Sec security protocols
- ISDN Cascade
- Serial connection
- Modem connection
- MPM cards
- QoS with IPv6
- Recording link
- SIP
- SIP security (Digest)
- SIP TLS
- SNMP
- SSH server.
- USB key configuration
- Web link (Hyperlink in Participant Properties dialog box)

Workstation Requirements

The *RMX Web Client* and *RMX Manager* applications can be installed in an environment that meets the following requirements:

- **Minimum Hardware** – Intel® Pentium® III, 1 GHz or higher, 1024 MB RAM, 500 MB free disk space.
- **Workstation Operating System** – Microsoft® Windows® XP, Vista®.
- **Network Card** – 10/100 Mbps.
- **Web Browser** – Microsoft® Internet Explorer® Version 7 only.
- **FIPS** – Is always enabled in *Ultra Secure Mode*, and when *ClickOnce* is used to install RMX Manager, the workstation must have one of the following installed:
  — *.NET Framework 3.5* or a later version of the *.NET Framework.*
  — *.NET Framework 2.0* plus *Service Pack 1* or later.

.Net Framework 2.0 is required and installed automatically.
The RMX must be installed on the intranet or added to the trusted sites list. In both cases, the ActiveX control will install properly.

Version 7.5.0.J - Upgrade Package Contents

The Version 7.5.0.J upgrade package must be downloaded from the *Polycom Resource Center* and includes the following items:

- lan.cfg file
- LanConfigUtility.exe
- RMX Documentation
  - RMX 1500/2000/4000 Version 7.5.0.J Release Notes for Maximum Security Environments
  - RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments
  - RMX 1500/2000/4000 Administrator's Guide for Maximum Security Environments
  - RMX 1500/2000/4000 Hardware Guides
  - RMX Third Party Licenses
- External DB Tools
  - RMX 1500/2000/4000 External Database API Programmer's Guide Sample Scripts

Connections to external databases are not supported in *Ultra Secure Mode*.

- RMX XML API Kit Version 7.5.0.J
  - RMX 1500/2000/4000 XML API Version 7.0.2 Release Notes
  - RMX 1500/2000/4000 XML API Overview
  - RMX 1500/2000/4000 XML API Schema Reference Guide (version 3.0)
  - MGC to RMX XML API Conferencing Comparison
  - Polycom XML Tracer User's Guide
  - XML Schemas
  - Polycom XML Tracer application

Version 7.5.0.J - Upgrade Procedure

> To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each LAN connection.

Upgrade Paths to Version 7.5.0.J

The upgrade options from previous versions to Version 7.5.0.J are summarized in Table 5.

Table 9   *Upgrade Paths to Version 7.5.0.J*

Current Version	First Intermediate Upgrade		Second Intermediate Upgrade		New Version	
	Version	**Key**	**Version**	**Key**	**Version**	**Key**
7.0.2	N/A		N/A		**7.5.0.J**	Yes
5.0.2	7.0.2	Yes	N/A		**7.5.0.J**	Yes
5.1	5.0.2	No	7.0.2	Yes	**7.5.0.J**	Yes

Upgrading from Version 7.0.2 to Version 7.5.0.J

1   Download the *Version 7.5.0.J* software from the *Polycom Resource Center* web site.

> If *Windows7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 7.5.0.J* software to the workstation.
> For more information see "*Windows 7™ Security Settings"* on page **16**.

2   Obtain the *Version 7.5.0.J Product Activation Key* from the *Polycom Resource Center* web site.

3   Backup the configuration file.

4   Install *MCU* Software *Version 7.5.0.J*.
On the *RMX* menu, click **Administration> Software Management > Software Download**.

5   *Browse* to the *Install Path,* selecting the **Version 7.5.0.J.x.x.bin** file in the folder where *Version 7.5.0.J* is saved and click **Install**.

The *Install Software* information box that the file *Copying files* is *In progress*.
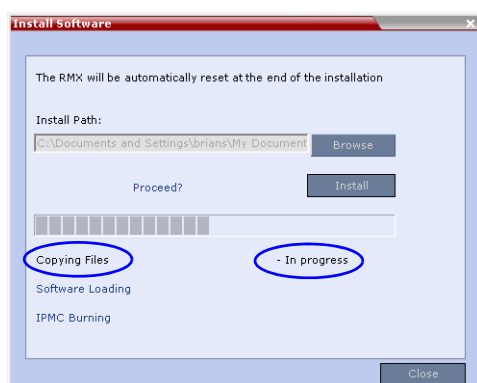
At the end of the installation process the system displays an indication that the software copying procedure is *Completed* and that a new *Activation Key* is required.

6   Click the **OK** button.

7   On the *RMX* menu, click **Setup > Product Activation**.

The *Product Activation* dialog box is displayed with the serial number field completed.

8   In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click the **OK** button.

At the end of the *Product Activation* process the system displays an indication that the *Product Activation Key* was successfully installed.

9   Click the **OK** button.

The *Install Software* information box indicates that *Software Loading* is in progress.

A series of *Active Alarms* are displayed indicating the progress of the upgrade process.

The *Install Software* information box indicates that *IPMC Burning* is in progress.

A further series of *Active Alarms* are displayed indicating the progress of the upgrade process.

Sometimes, when updating the *Version 7.x* license key, the system displays the following active alarm:

Ignore this Active Alarm and complete this installation procedure.

The upgrade procedure takes approximately **20** minutes.

Connection to the *RMX* is terminated and you are prompted to reopen the browser.

10 Approximately 5 minutes after receiving this message, close and reopen the browser.

11 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RMX*.

The browser displays a message indicating that it cannot display the requested page.
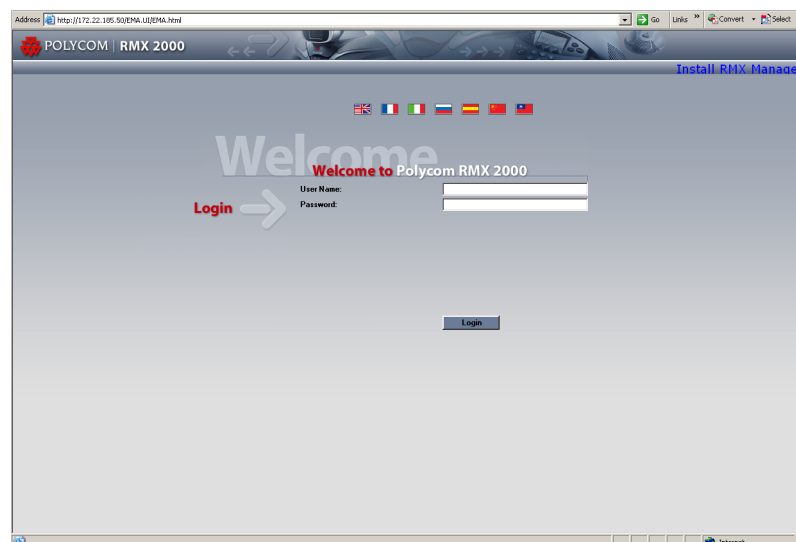
12 In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

25

In the *Main Screen* an *MCU State* indicator displays a progress indicator
`Starting up (15:25)` showing the time remaining until the system start-up is complete.

> • If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until a new Administrator user is created and the default user is deleted.
> • If the upgrade process fails, please contact Polycom support.

13 To use the new features such as *Operator Assistance* and *Gateway Sessions* the *IVR Services* must be updated. For more details, see *"Additional/Optional System Updates After Upgrading"* on page **20**.

Upgrading from Version 5.0.2 to Version 7.5.0.J

This upgrade requires an intermediate upgrade from *Version 5.0.2* to *Version 7.0.2* followed by an upgrade to *Version 7.5.0.J*.

Intermediate Upgrade from Version 5.0.2 to Version 7.0.2

1 Download the software **Version 7.0.2** software from the *Polycom Resource Center* web site.

> If *Windows7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 7.0.2* software to the workstation.
> For more information see "*Windows 7™ Security Settings"* on page **16**.

2 Obtain the Version 7.0.2 *Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX Getting Stated Guide*, "*Procedure 1: First-time Power-up"* on page **2-22**.

3 Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide, "Software Management"* on page **19-111**.

4 Install *MCU* Software Version 7.0.2.
On the *RMX* menu, click **Administration > Software Management > Software Download**.

5 *Browse* to the *Install Path,* selecting the **Version 7.0.2xx.bin** file in the folder where **Version 7.0.2**. is saved and click **Install**.

At the end of the installation process the *Install Software* dialog box indicates that the installed software is being checked. The system then displays an indication that the software was successfully downloaded and that a new activation key is required.

6 On the *RMX 2000/4000* menu, click **Setup > Product Activation**.

The *Product Activation* dialog box is displayed with the serial number field completed.
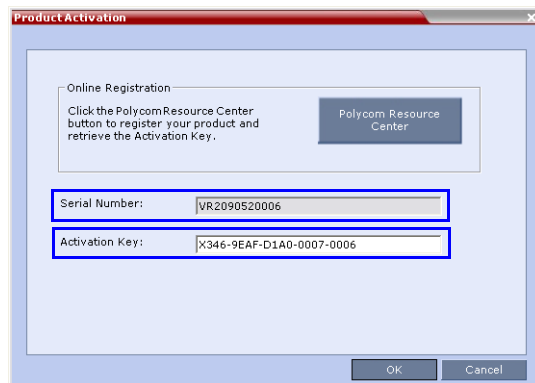
7 In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click the **OK** button.

At the end of the *Product Activation* process the system displays an indication that the *Product Activation Key* was successfully installed.

8 When prompted whether to reset the *RMX*, click **Yes** to reset the *RMX*.

> Sometimes when upgrading from version 5.0.2 to version 7.0.x the reset process fails. In such a case, you can try to connect to the *MCU* via the Shelf Management and reset the *MCU* from the Hardware Monitor or you can "hard" reset the *MCU* by turning the Power off and on again.

9 When prompted to wait while the *RMX* resets, click **OK**.

The upgrade procedure takes approximately 30 minutes.

Connection to the *RMX* is terminated and you are prompted to reopen the browser.

10 After approximately 30 minutes close and reopen the browser.

11 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RMX*.

The browser displays a message indicating that it cannot display the requested page.

12 Refresh the browser periodically until connection to the *RMX* is established and the *Login* screen is displayed.

You may receive a message stating *Browser environment error. Please reopen the browser.*

13 **Optional.** Close and reopen the browser.

14 Enter the IP address of the *RMX Control Unit* in the browser's address line and press **Enter** to reconnect to *RMX*.

The *Login* screen is displayed. The version number has changed to *7.0.2.*
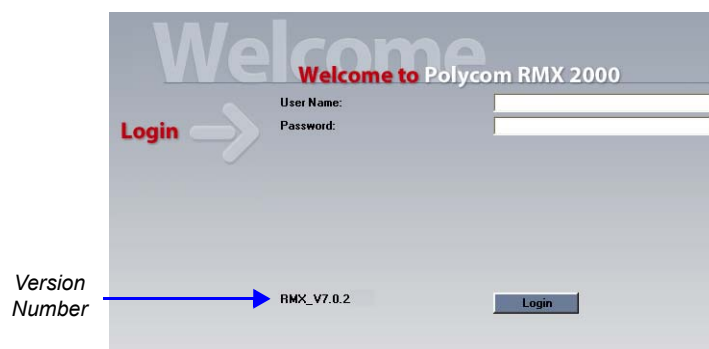
15 In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator
Starting up (15:25) showing the time remaining until the system start-up is complete.

- If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until a new Administrator user is created and the default user is deleted.
- If the upgrade process fails, please contact Polycom support.

Upgrade from Version 7.0.2 to Version 7.5.0.J

>> Continue with the upgrade from *Version 7.0.2* to *Version 7.5.0.J* as described starting on page **23**.

To use the new features such as *Operator Assistance* and *Gateway Sessions* the *IVR Services* must be updated. For more details, see *"Additional/Optional System Updates After Upgrading"* on page **20**.

Upgrading from Versions 5.1.0.G to Version 7.5.0.J

This upgrade requires the following intermediate upgrade procedures followed by an upgrade to *Version 7.5.0.J*:

1 Upgrade from *Version 5.1.0.G* to *Version 5.0.2*.
2 Upgrade from *Version 5.0.2* to *Version 7.0.2*.

Intermediate Upgrade from Version 5.1.0.G to Version 5.0.2

Ultra Secure Mode must be disabled before this upgrade can be performed.

1 Download the required software *Version 5.0.2* from the *Polycom Resource Center* web site.

If *Windows7™* is installed on the workstation, *Protected Mode* must be disabled before downloading the *Version 5.0.2* software to the workstation.
For more information see *"Windows 7™ Security Settings"* on page **16**.

---

2   Backup the configuration file. For more information, see the *RMX 1500/2000/4000 Administrator's Guide, "Software Management"* on page **19-111**.

3   Install *MCU* Software *Version 5.0.2*.
On the *RMX* menu, click **Administration> Software Management > Software Download**.

4   *Browse* to the *Install Path,* selecting the **Version 5.0.2xx.bin** file in the folder where *Version 5.0.2* is saved and click **Install**.

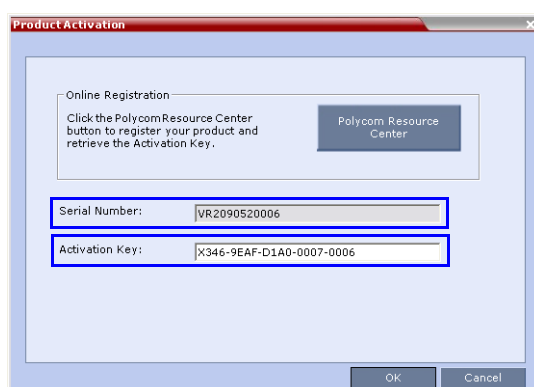At the end of the installation process the system displays an indication that the software was successfully downloaded and that a new activation key is required.

5   Click **Close** to close the *Install Software* dialog box.

6   When prompted whether to reset the *MCU*, click **Yes** to reset the *MCU*.

At the end of the installation process the system displays an indication that the software was successfully downloaded.

The upgrade procedure takes about **30** minutes during which time an *Active Alarm - System Upgrade* is displayed.

The RMX resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP.*

7   After about **30** minutes, **close and reopen the browser** and connect to the RMX. If the browser was not closed and reopened, the following error message is displayed: "Browser environment error. Please reopen the browser".

The version number in the *Welcome* screen has changed to *5.0.2*.
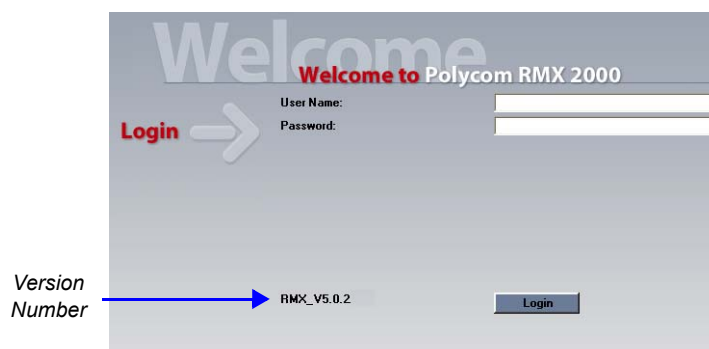
8   In the *RMX Web Client – Welcome* screen, enter your *User Name* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator showing the time remaining until the system start-up is complete.

Intermediate Upgrade from Version 5.0.2 to Version 7.0.2

>>   Continue with the upgrade from *Version 5.0.2* to *Version 7.0.2* as described starting on page **26**.

Upgrade from Version 7.0.2 to Version 7.5.0.J

>>   Continue with the upgrade from *Version 7.0/7.0.1/7.0.2* to *Version 7.5.0.J* as described starting on page **23**.

To use the new features such as *Operator Assistance* and *Gateway Sessions* the *IVR Services* must be updated. For more details, see *"Additional/Optional System Updates After Upgrading"* on page 20.

Detailed Description - RMX 1500

The Polycom® RMX® 1500 supports multiple network protocols - IP (H.323, SIP), PSTN, and ISDN - to extend the power of unified collaboration within the enterprise.

The RMX® 1500 user and administrator interface is the same as for the RMX 2000/4000.

The RMX 1500 Real-time Media Conference platform offers up to 90 video resources and 360 audio resources. For detailed description of the RMX 1500 hardware components, see the *Polycom RMX 1500 Hardware Guide*.

Card Configuration Mode

The RMX 1500 operates in the *MPMx Card Configuration Mode*.

System Capacities

Conferencing Capacities

The following table summarizes the different conferencing capacities:.

Table 1-1   System Functions and Capacities RMX 1500

System Functions	Capacity
Maximum number of Video participants in a conference	90
Maximum number of PSTN participants in a conference	120
Maximum number of VOIP participants in a conference	360
Maximum number of Audio calls per second	5
Maximum number of Video calls per second	2
Maximum number of Conferences	400
Maximum number of Meeting Rooms	1000
Maximum number of Entry Queues	40
Maximum number of Profiles	40
Maximum number of Conference Templates	100
Maximum number of SIP Factories	40
Maximum number of IP Services	1
Maximum number of ISDN Services	2
Maximum number of IVR Services	40
Maximum number of Recording Links	20 (default)
Maximum number of IVR Video Slides	150
Maximum number of Log Files (1Mb max.)	4000
Maximum number of CDR Files	2000

Table 1-1   System Functions and Capacities RMX 1500

System Functions	Capacity
Maximum number of Fault Files	1000
Number of Participant alerts	Unlimited
Maximum number of concurrent RMX Web Client connections to the MCU	20
Maximum number of Users	100
Maximum number Address Book entries	4000
Maximum number of gateway profiles	40
Maximum number of Reservations (Internal Scheduler)	2000

Resource Capacities

The following table summarizes the resource capacities according to audio, video and video resolutions in CP conferences:.

Table 1-2   System Resource Capacities per Audio or Video and Resolution in CP Conferences

Audio/Video and Resolution	RMX 1500 (MPMx) Resources
HD Support	CP / VSW
PSTN	120
VOIP	360
ISDN	60 (128 Kbps) - 4 E1/T1
CIF H.263	60
CIF H.264	90
SD / 4CIF H.264	60
4CIF H.263	30
720p30	30
1080p30fps/720p60	15 (Symmetric)

The following table summarizes the resource capacities according to line rates in VSW conferences as line rates are deciding factor:.

Table 1-3   System Resource Capacities per Line Rate in VSW conferences

Audio/Video and Resolution	RMX 1500 (MPMx) Resources
VSW 2Mb	80
VSW 4Mb	40
VSW 6Mb	20

Network Connectivity

On the RMX 1500 Media and Signaling are on the same network, but have separate IP addresses. However, Management of the RMX is separate network from Media & Signaling.

All IP addresses have separate physical LAN connector.

Power Cable   *E1/T1 PRI Connection(s)*   LAN 2; media, *MNG; signaling, MNGB; management & Shelf*
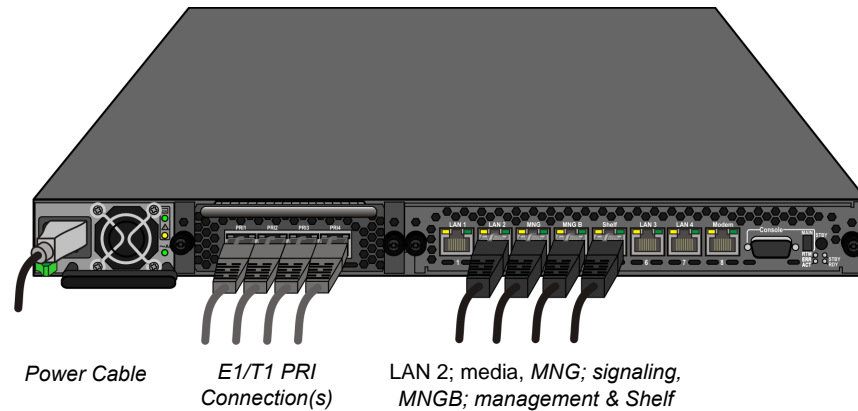
RMX 1500 Rear Panel View with AC Power and Communication Cables

Hardware Monitoring

In the RMX 1500, component information can be viewed in the *Hardware Monitor* section.
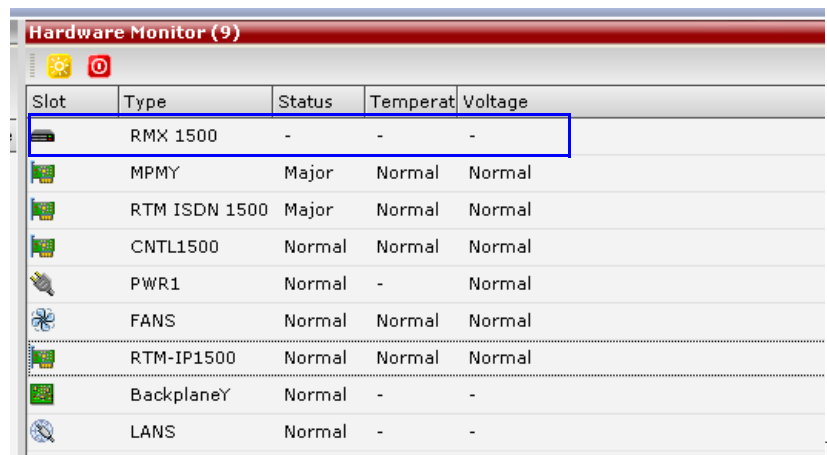
The properties displayed for the hardware components will vary according to the type of component viewed. These component properties

can be grouped as follows:

- MCU Properties (RMX 1500)
- Card Properties (RTM IP 1500, RTM ISDN)
- Supporting Hardware Components Properties (MPMx, Backplane, FANS, LAN)

Hardware Monitor - Slot Components

On the RMX 1500, each internal component can be viewed via the Hardware Monitor.

Table 2   *RMX 1500 Slot Components*

Card/Component	Requirement
MPMx Media Card	(Internal Component). Build-in MPMx card. The internal media card requires the RTM IP 1500 card.
RTM ISDN 1500	(Optional) ISDN card for 4 E1/T1 connections. This card is field replaceable.
CNTL 1500	(Internal Component). Internal Management of the system.
Power Supply	Mandatory. Supplies AC Power to the RMX. This unit is not field replaceable.
Fan (Internal Component)	(Internal Component). Provides cooling for the internal RMX components.
RTM-IP 1500	Mandatory. Contains an Ethernet Switch that manages the network of the system, routes data between the cards and components of the system and provides connectivity to external IP networks. This unit is not field replaceable.
BackplaneY	(Internal Component). Data Routing.
LANS	(Internal Component). Provide Network access.

RMX 1500 Properties

The *RMX 1500 Properties - General Info* tab.
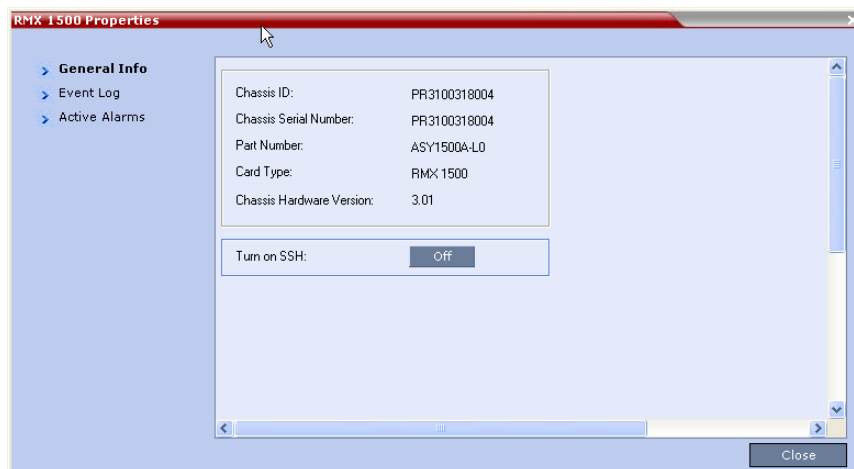
CNTL 1500 Properties

The *CTRL_PLUS Properties - General Info* tab.
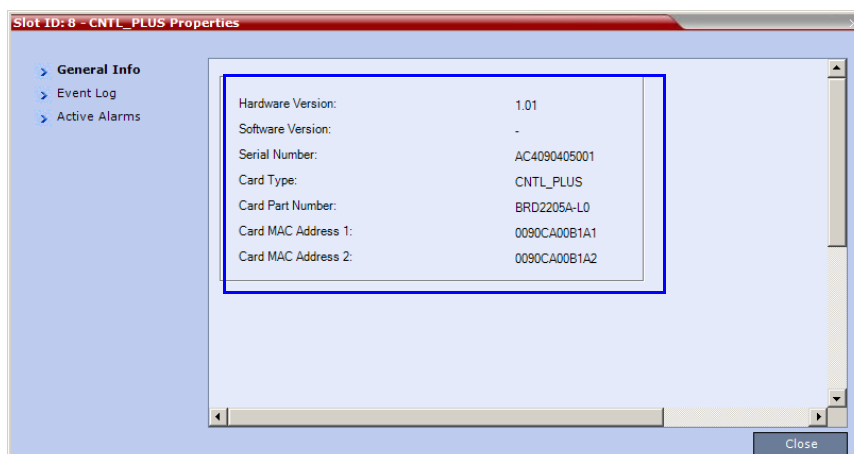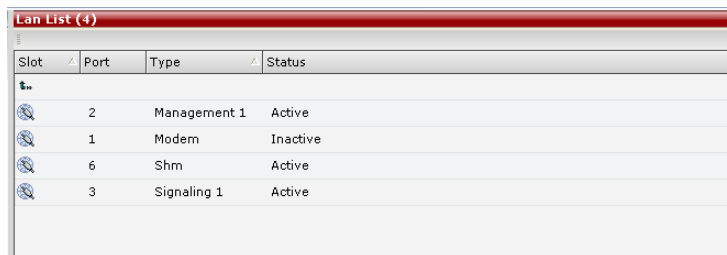
RTM IP 1500 Properties

The *RTM IP Properties - General Info* tab.
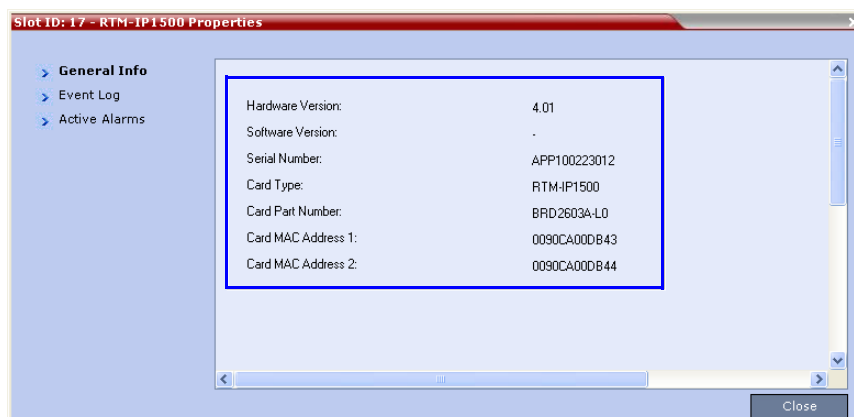
LAN Unit List Properties
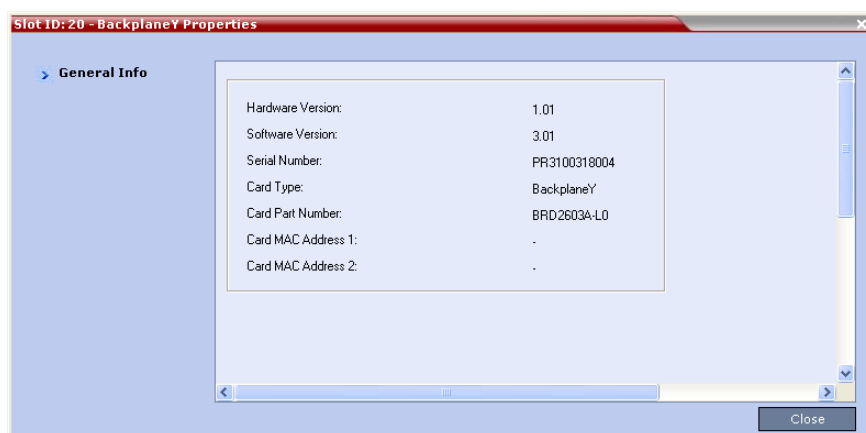
The *LAN Unit List* Properties.

Slot	Port	Type	Status
	2	Management 1	Active
	1	Modem	Inactive
	6	Shm	Active
	3	Signaling 1	Active

Lan List (4)

Backplane 1500 Properties
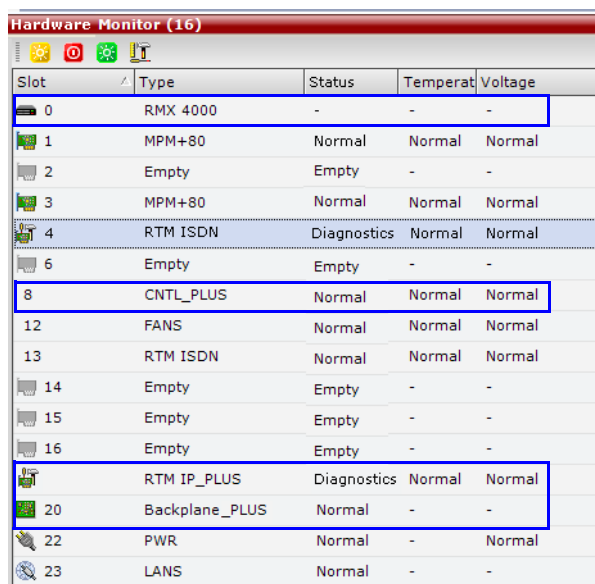
The *Backplane_PLU Properties - General* Info tab.

Slot ID: 20 - BackplaneY Properties

> **General Info**

Hardware Version:	1.01
Software Version:	3.01
Serial Number:	PR3100318004
Card Type:	BackplaneY
Card Part Number:	BRD2603A-L0
Card MAC Address 1:	-
Card MAC Address 2:	-

Close

Hardware Monitor Component Diagnostics

In the *Hardware Monitor Diagnostics* pane, new components are added to the UI:

Hardware Monitor (16)

Slot	Type	Status	Temperat	Voltage
0	RMX 4000	-	-	-
1	MPM+80	Normal	Normal	Normal
2	Empty	Empty	-	-
3	MPM+80	Normal	Normal	Normal
4	RTM ISDN	Diagnostics	Normal	Normal
6	Empty	Empty	-	-
8	CNTL_PLUS	Normal	Normal	Normal
12	FANS	Normal	Normal	Normal
13	RTM ISDN	Normal	Normal	Normal
14	Empty	Empty	-	-
15	Empty	Empty	-	-
16	Empty	Empty	-	-
	RTM IP_PLUS	Diagnostics	Normal	Normal
20	Backplane_PLUS	Normal	-	-
22	PWR	Normal	-	Normal
23	LANS	Normal	-	-

New components have been added to the *Hardware Monitor - Diagnostics Test* pane:
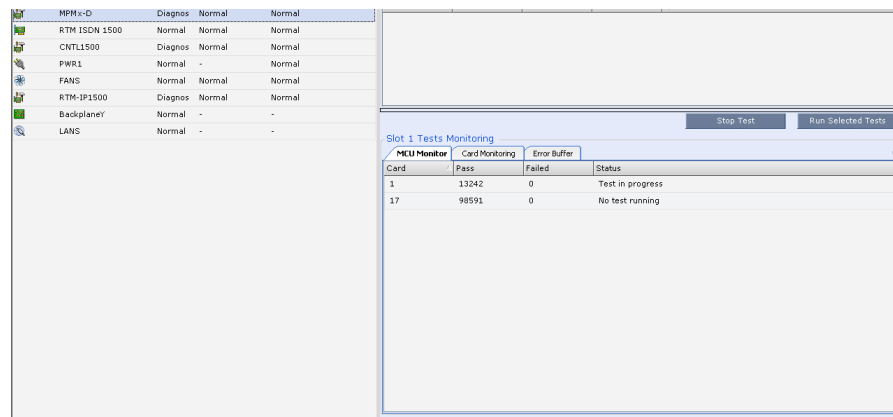
Video/Voice Port Configuration and Resource Report Changes

No reset is required when changing the *Video/Voice Port Configuration* on the RMX 1500.

When switching between *Flexible Resource Capacity* and *Fixed Resource Capacity* modes, no reset is required. However, the Video/Voice Configuration slider cannot be changed while there are ongoing conferences on the RMX 1500.

> *Flexible Resource Capacity* is default resource allocation mode on the RMX 1500.

The Video and Audio resource capacities on the RMX 1500 are a maximum of:

* 90 Video Ports
* 360 Audio Ports
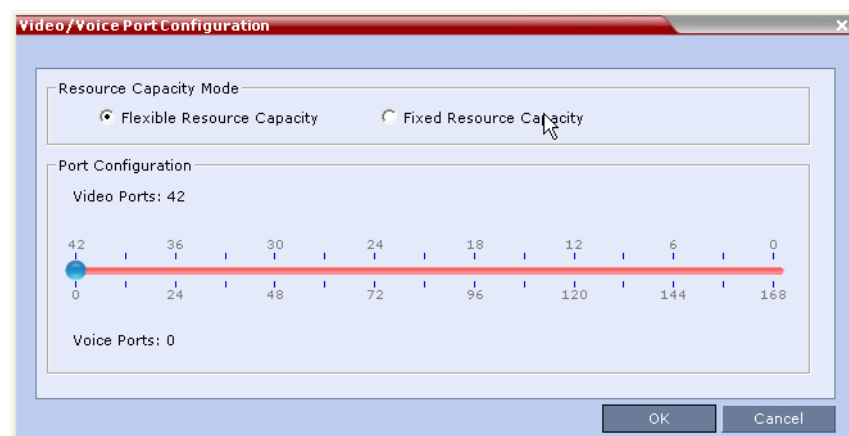
The *Resource Capacity Mode*s are identical to the RMX 2000/4000.

The slider moves in multiples of three (in *MPMx Card Configuration Mode)*, converting CIF video ports to voice ports in groups of three, with each CIF video port converting to four voice ports. The minimum number of voice ports that can be allocated is 12 (3 video ports x 4 voice ports per video port).

Resource Report

The resource capacity of RMX 1500 can be viewed in the Resource Report pane:
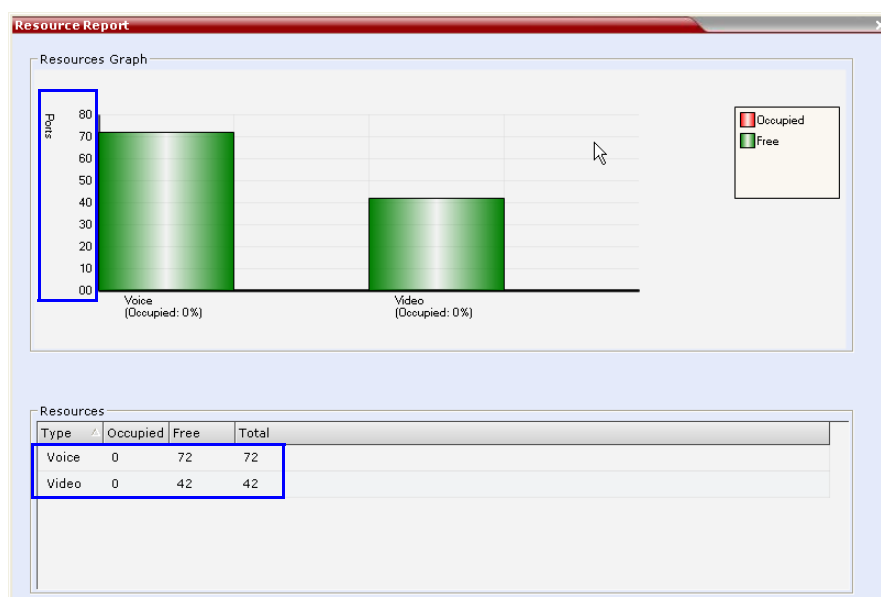
It reflects the MPMx card assembly type (MPMx-S and MPMx-D) and the Resource Allocation Mode (Flexible or Fixed).

MCU Type Indication

RMX 1500 Banner

The RMX model (RMX 2000/RMX 4000/RMX 1500) is indicated in the RMX Web Client banner and in the Welcome heading.
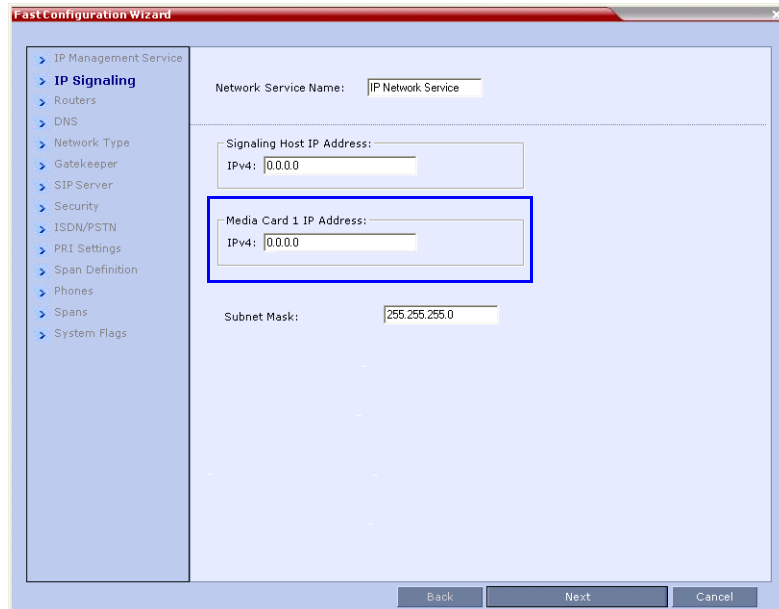
RMX Manager Application

In the *RMX Manager* application, the RMX 1500 is indicated in the MCU Type and the appropriate MCU icon is displayed when the RMX 1500 is defined .

Network Service Changes

Fast Configuration Wizard - RMX 1500

The *Fast Configuration Wizard - IP Signaling* tab is available on the RMX 1500. A single IP Address field for the MPMx media card is added to the *IP Signaling Tab*.

Detailed Description - MPMx Media Card

RMX Version 7.0.x supports the latest *MPMx (*Media Processing Module) card which increases the RMX's capacity and capabilities.

When *MPMx* cards are installed, the RMX operates in *MPMx Mode* giving the administrator enhanced control and monitoring of *Resource Capacity* and usage within the system.

> MPMx cards are supported only with **D-type** chassis and software version 7.0.x.

Front Panel & LEDs

In terms of Look and Feel and LED functionality, the MPMx front panel is identical to the MPM+.

Conferencing Capacities

Table 3 lists the maximum conferencing capacities of *RMX 4000*, *RMX 2000* and *RMX 1500* when used with *MPMx* cards.

Table 3   *MPMx Capacities - RMX 4000/2000/1500*

Maximum Number of:	RMX4000	RMX2000	RMX1500
Video Participants in a Conference	180	180	90
Conferences	800	400	400
Meeting Rooms	2000	1000	1000
Entry Queues	80	40	40
Profiles	80	40	40
Conference Templates	200	100	100
SIP Factories	80	40	40
IP Services	1	1	1
ISDN Services	2	2	2
IVR Services	80	40	40
Recording Links	20	20	20
IVR Video Slides	150	150	150
Reservations (Internal Scheduler)	4000	2000	2000
Log Files (1Mb max.)	8000	4000	4000
CDR Files	4000	2000	2000
Fault Files	1000	1000	1000

Table 3   *MPMx Capacities - RMX 4000/2000/1500 (Continued)*

Maximum Number of:	RMX4000	RMX2000	RMX1500
Number of Participant alerts	*Unlimited*	*Unlimited*	*Unlimited*
HTTP (Web) clients connected to the MCU	*20*	*20*	*20*
Address Book entries	*4000*	*4000*	*4000*
Users	*100*	*100*	*100*

Resource Capacities

Resource Capacities per Card Assembly

The MPMx can be shipped in two card assemblies. Table 2 summarizes the video capacities of the two *MPMx* card assemblies per resolution in CP conferencing.

Table 4   *MPMx Resource Capacity per Card – CP Conferencing*

Resource Type	MPMx - S	MPMx - D
Voice	180	360
H.263 CIF	30	60
H.263 4CIF15	15	30
H.264 CIF	45	90
SD H.264	30	60
HD720p30	15	30
HD720p60/ HD1080p30	8	15 (Symmetrical)

Table 5 summarizes the video capacities of the two *MPMx* card assemblies per line rate in VSW conferencing.

Table 5   *MPMx Resource Capacity per Card – VSW Conferencing*

Resource Type	MPMx - S	MPMx - D
VSW 2Mbps	40	80
VSW 4Mbps	20	40
VSW 6Mbps	10	20

Resource Capacities per Card Type (MPM+ and MPMx)

Each *MPMx* card increases the resource capacities. HD720p60 and *HD1080p30* symmetric resolutions are now supported with MPMx.

Table 4 summarizes resource capacities of the various cards that can be installed in an RMX per resolution in CP conferencing (resolution being the deciding factor) .

Table 6   *MPMx and MPM+ – Resource Capacity per Resolution - CP Conferencing*

Resource Type	Maximum Possible Resources Per Card	
	MPM+	MPMx
HD720p60/HD1080p30 Symmetric	Not Applicable	15
HD720p60/HD1080p30 Asymmetric	10	15
HD720p30	20	30
SD 60	20	30
SD 30 (H.264)	30	60
4CIF 60	20	30
4CIF 30 (H.263)	30	30
CIF 60 (H.264)	30	60
CIF 30 (H.264)	80	90
CIF (H.263)	80	60
Audio only (VoIP)	400	360

Table 6 summarizes resource capacities of the various cards that can be installed in an RMX per line rate in VSW conferencing (line rate being the deciding factor) .

Table 7   *MPMx and MPM+ – Resource Capacity per Resolution - VSW Conferencing*

Resource Type	Maximum Possible Resources Per Card	
	MPM+	MPMx
VSW 2Mbps	80	80
VSW 4Mbps	40	40
VSW 6Mbps	20	20

Total Resource Capacities per System

Table 8 lists the maximum resource capacities of *RMX 4000, RMX 2000* and *RMX 1500* per resolution in CP Conferencing mode when used with *MPMx* cards.

Table 8   *MPMx Resource Capacities - RMX 4000/2000/1500*

Maximum Number of:	RMX4000	RMX2000	RMX1500
CIF Resources	360	180	90
H.264 SD Resources	240	120	60
H.263 4CIF Resources	120	60	30

Table 8　　*MPMx Resource Capacities - RMX 4000/2000/1500 (Continued)*

Maximum Number of:	RMX4000	RMX2000	RMX1500
HD 720p 30fps Resources	*120*	*60*	*30*
HD 720p 60fps Resources	*60*	*30*	*15*
HD 1080p 30 fps Resources	*60*	*30*	*15*
PSTN Audio Resources	*400*	*400*	*120*
VoIP Audio Resources	*1440*	*720*	*360*

Table 9 lists the maximum resource capacities of *RMX 4000, RMX 2000* and *RMX 1500* per line rate in VSW conferencing (line rate being the deciding factor) when used with *MPMx* cards.

Table 9　　*MPMx, MPM+ – Resource Capacity per Resolution - VSW Conferencing*

Resource Type	Maximum Possible Resources Per Card		
	RMX4000	RMX2000	RMX1500
VSW 2Mbps	320	160	80
VSW 4Mbps	160	80	40
VSW 6Mbps	80	40	20

Audio Algorithm Support

In addition to the standard audio algorithms, the MPMx card also supports Polycom's proprietary *Siren 22* and industry standard *G.719* audio algorithms for participants connecting with *Polycom* endpoints.

For more details, see the *RMX 1500/2000/4000 XYZ Guide, "Audio Algorithm Support"* on page **2-60**.

MPMx Guidelines

MPMx and MPM+ Modes

- **MPMx Mode** is the mode in which the RMX operates to fully utilize the increased power and capacity of *MPMx* cards.

MPMx and MPM+ cards that are installed in the system **cannot be used simultaneously**.
The RMX can operate in **either** *MPM+* **or** *MPMx* mode.

- ISDN support is the same as for MPM+ cards.

Operating Mode Selection During Startup / Restart

- When started with Version 7.0.x installed, the RMX enters *MPMx Mode* by default when no media cards are installed.

- The RMX switches between *MPMx* and *MPM+ Card Configuration Modes* when *MPM+/MPMx* cards are removed or swapped while the system is running.
- The switch between *Card Configuration Modes* occurs during the **next** restart.
- Installing or swapping *MPM+/MPMx* cards while the system is off will not cause a switch in the *Card Configuration Mode* when the system is restarted – it will restart in the *Card Configuration Mode* that was active previous to powering down.

System Information Changes

The *System Information* includes *License Information*, and general system information, such as system memory size and *Media Card Configuration Mode*, which in version 7.0.x includes the *MPMx Mode*.

Table 10 summarizes the *Operating Mode After Next Restart* resulting from of adding or swapping *MPM+/MPMx* cards in a running system .

Table 10 RMX Card Configuration Mode After Next Restart

Current Operating Mode	Media Cards Installed	Card(s) Supported	Card(s) Disabled	Operating Mode After Next Restart
MPMx	MPM+	None	All	MPM+
	MPM+ and MPMx	MPMx Only	MPM+	MPMx
MPM+	MPM+	All	None	MPM+
	MPM+ and MPMx	MPM+ Only	MPMx	MPMx

Example:

Current status

An RMX has *MPM+* card installed.

The *Card Configuration Mode* is **MPM+**.

and the *MPM+* card is **enabled**.

Action

- Insert one *MPMx* card.

Result

- The *Card Configuration Mode* remains **MPM+**.
- *MPM+* card is **enabled.**
- The inserted *MPMx* card is **disabled**.

After Reset
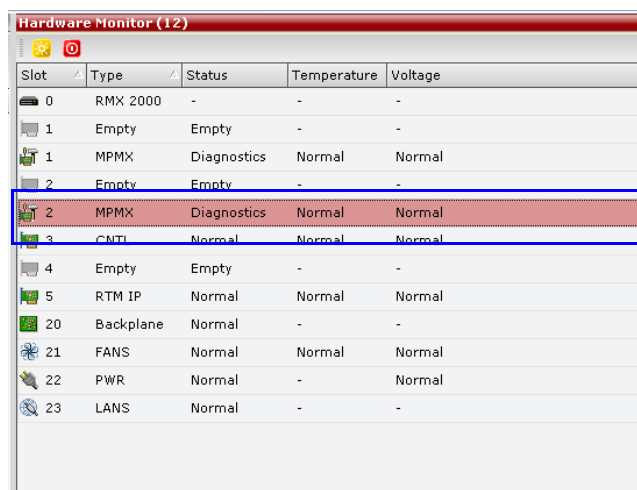
The *Card Configuration Mode* is **MPMx**.

The inserted *MPMx* card is **enabled**.

The remaining *MPM+* card (if not removed) is **disabled**.

MPMx Hardware Monitoring

The status and properties of the MPMx Card can be viewed and monitored in the Hardware Monitor list pane. The Hardware monitor pane displays the type(s) of MPM+/MPMx card installed on the *RMX 1500/2000/4000*. For more information, see the *RMX 1500/2000/4000 Administrator's Guide, "RMX Hardware Monitoring"* on page **20-1**.

MPMx Hardware Diagnostics

Diagnostics can be performed on the MPMx card(s) when the MCU is in *Diagnostics* mode.

To Monitor the MPMx Card:

• In the Hardware Monitor pane select the *MPMx* card and click **Diagnostics** from the drop-down menu. For more information, see the *RMX 1500/2000/4000 Administrator's Guide, "Diagnostic Mode (RMX 1500/2000/4000)"* on page **20-31**.

Video/Voice Port Configuration

The *System Card Configuration Mode* determines the resource allocation method used by the RMX to allocate resources to the connecting endpoints. As with *MPM+ Card Configuration Mode*, both **Flexible Resource Capacity™** and **Fixed Resource Capacity™** are available in *MPMx Card Configuration Mode*.

• In *MPMx Card Configuration Mode* the slider moves in multiples of three, converting CIF video ports to voice ports in groups of three, with each CIF video port converting to four voice ports. The minimum number of voice ports that can be allocated is 12 (3 video ports x 4 voice ports per video port).

• The first time the *Fixed Resource Capacity* is selected, all resources are allocated to HD720p30 by default.

• If the *Resource Capacity Mode* was previously *Fixed* or if it was *Flexible* but *Fixed* had been selected in the past, the previous resource allocations in the mode are displayed.

> CIF H.263 endpoint connections require more resources than CIF H.264 - they require the same amount as SD connections. Therefore, when Fixed Mode is used for resource allocation, SD resources must be configured to ensure that H.263 endpoints can connect with video.

For more information about *Video/Voice Port Configuration*, see *RMX 1500/2000/4000 Administrator's Guide*, *"Video/Voice Port Configuration"* on page **19-59**.

MPMx Resource Report

The *Resource Report* displays the real time resource usage according to the *Card Configuration Mode* and the selected *Resource Capacity Mode*.

For more details about Resource Report, see the *RMX 1500/2000/4000 Administrator's Guide*, *"Resource Report"* on page **19-68**.

Port Gauges

Audio (*Voice*) resources are as displayed as in previous versions while all *Video* resource types are shown as a single group of *Video* resources.

Port Usage: Voice   0 / 18   Video   4 / 47
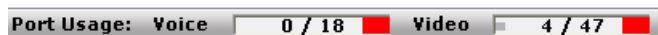
For more details, see the *RMX 1500/2000/4000 Administrator's Guide*, *"Port Usage Gauges"* on page **19-77**.

Detailed Description - New Security Features

(PKI) Public Key Infrastructure

PKI (*Public Key Infrastructure*) is a set of tools and policies deployed to enhance the security of data communications between networking entities.

Unique Certificates for all Networked Entities

The implementation of *PKI* on the *RMX* has been enhanced to ensure that all networked entities are checked for the presence of unique certificates by implementing the following rules and procedures during the *TLS* negotiation:

- The *RMX* identifies itself with the same certificate when operating as a server and as a client.

- The *RMX's* management applications: *RMX Web Client* and *RMX Manager*, identify themselves with certificates.

- While establishing the required TLS connection, there is an exchange of certificates between all entities.

- Entities such as *CMA* and *DMA* that function as both client and server within the *Management Network* identify themselves with the same certificate for both their client and server functions.

The following diagram illustrates the certificate exchange during the *TLS* connection procedure.
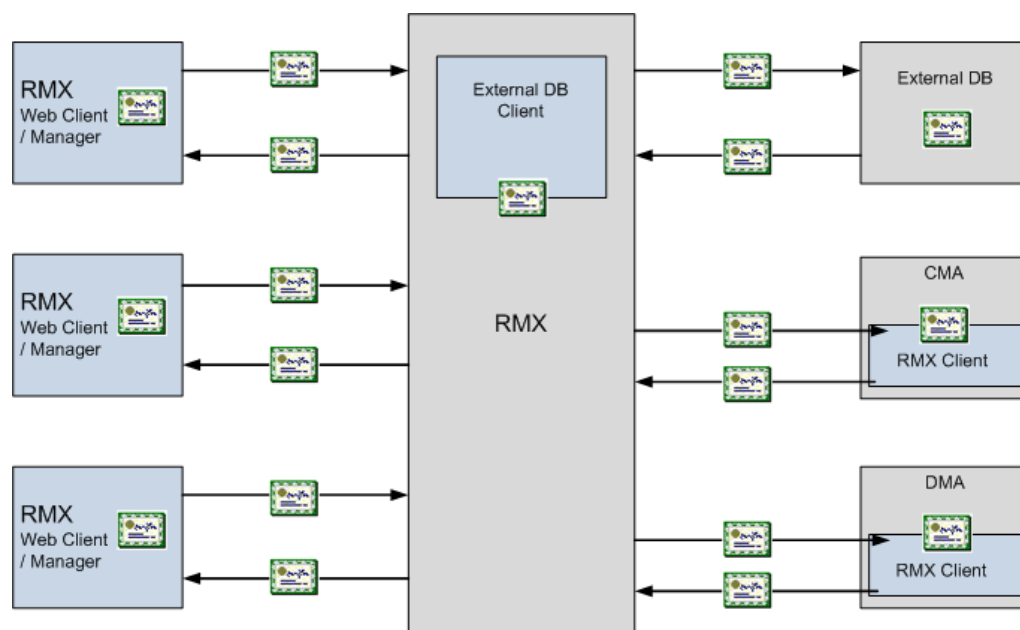
Offline Certificate Validation

Offline Certificate Validation has been enhanced to include the following rules and procedures:

Peer Certificates

The diagram below illustrates the peer certificate validation procedure.

- The credentials of each certificate received from a networked peer are verified against a repository of trusted certificates. (Each networked entity contains a repository of trusted certificates.)
- The digital signature of the certificate's issuing authority is checked along with the certificate's validity (expiration date).
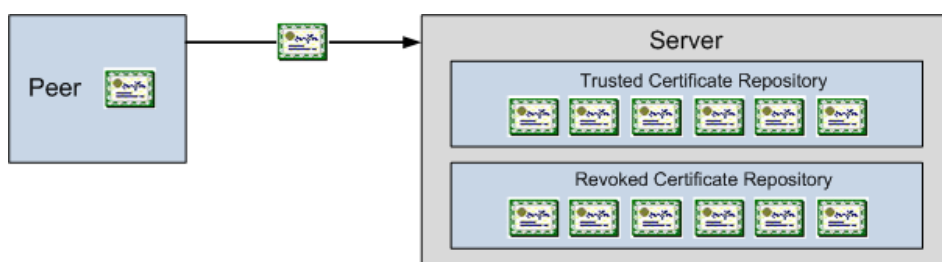
Self Validation of Certificates

- The *DNS* name field in the entity's certificate is checked for a match with the entity's *DNS* name.
- The date of the *RMX's* certificate is checked for validity during power-up and when connecting to management applications (*RMX Web Client* and *RMX Manager*).

Certificate Revocation List

- Each certificate received from a networked peer is verified against a repository of revoked certificates. (Each networked entity contains a repository of revoked certificates.
- Revocation certificates are checked against a list of trusted issuers.
- The digital signature of the issuing authority of the revocation certificate is verified.

Installing and Using Certificates on the RMX

The following certificate file formats are supported:

- *PEM*
- *DER*
- *PKCS#7/P7B*
- *PKCS#12PFX*

Default Management Network

The procedure necessary to purchase and install certificates for the *Default Management Network* of the *RMX* is unchanged and is described in the *RMX 1500/2000/4000 Administrator's Guide, "Secure Communication Mode"* on page **F-1**.

Enabling Peer Certificate Requests

A new tab, *Security*, has been added to the *Management Network Properties* dialog box to enable the *Request Peer Certificate* feature to be enabled

The *Request peer certificate* check box must be selected before enabling Secured Mode. If it is not selected an *Active Alarm* is created and a message is displayed stating that *Secured Communications Mode* must be enabled.

To enable Request Peer Certificate:
1   In the *RMX Management* pane, click the **IP Network Services** entry.
2   In the *IP Network Services* list pane, double-click the **Management Network** entry.
3   Click the **Security** tab**.**
4   Select the *Request Peer Certificate* check box.
5   Click the **OK** button.
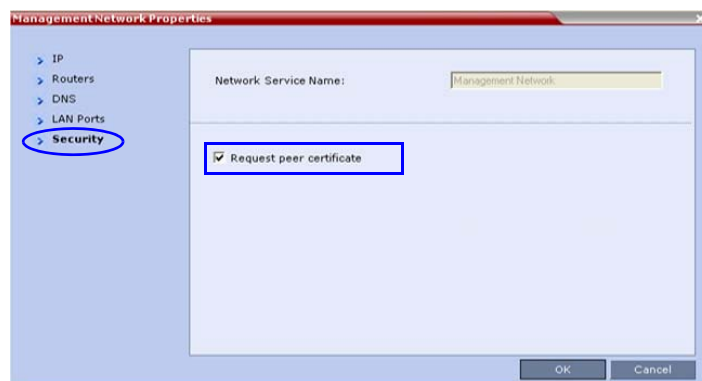
Default IP Network Service

The steps needed to add a certificate to the *Default IP Network Service* are described in the *RMX 1500/2000/4000 Administrator's Guide,"Modifying the Default IP Network Service"* on page **14-13**.
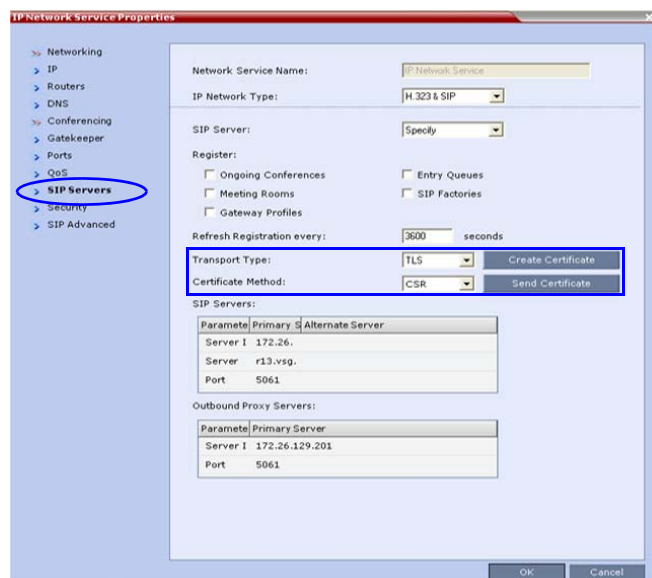
Managing Certificates in the Certification Repository

A *Certification Repository* dialog box has been added to enable the administrator to add remove and monitor certificates on the *RMX*. It is accessed via the *RMX Web Client /* RMX *Manager*, *Setup* menu.
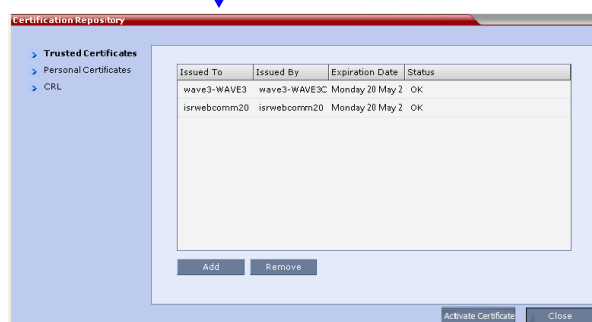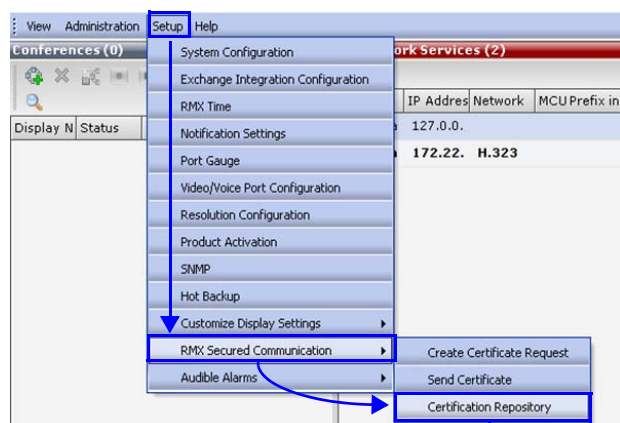
For information about purchasing certificates see the *RMX 1500/2000/4000 Administrator's Guide*, *"Purchasing a Certificate"* on page **F-1**.

The *Certification Repository* dialog box contains tabs that display the following lists:

- *Trusted Certificates*
- *Personal Certificates (Management and Signaling Certificates)*
- *CRL (Certificate Revocation List)*

Double-clicking on a certificate in any if the displayed lists, displays the certificate's properties:

Adding Trusted Certificates and CRLs to the Certification Repository

Trusted Certificates and *CRL*s added to the *Certification Repository* are not automatically activated. They remain in the *Trusted Certificates* and *CRL Lists* until the **Activate Certificate** button is clicked, at which time all *Trusted Certificates* and *CRLs* in the list are activated simultaneously.

Trusted Certificates

By clicking the column headers the *Trusted Certificates* can be sorted by:

- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*
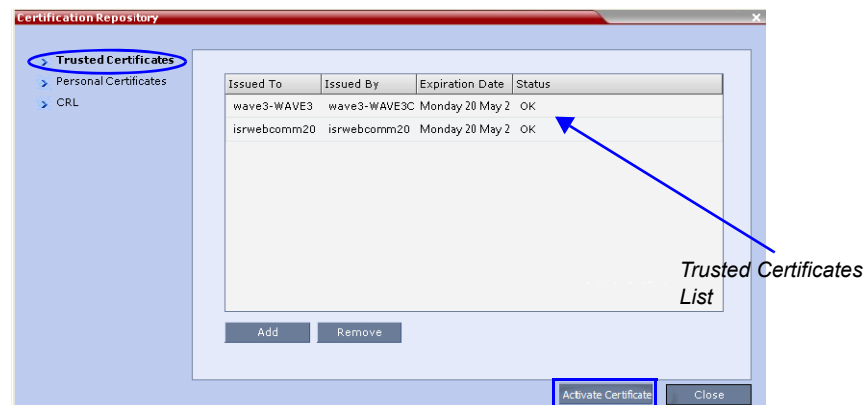
Adding Trusted Certificates

To add a certificate to the repository:

Repeat steps 1 - 4 for each certificate that is to be added to the *Certification Repository*.

1   In the *Trusted Certificates* tab click the **Add** button.

 The *Send Certificate* dialog box is displayed.
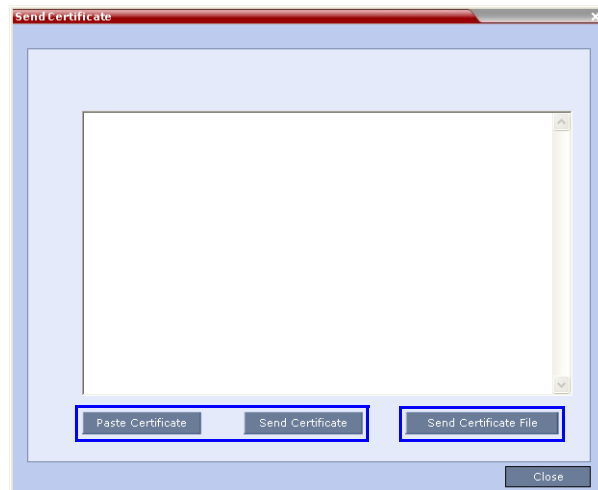
2   Send the certificate to the RMX.

 Two options are available for sending the certificate to the RMX:

 —   **Paste Certificate and Send Certificate**
 Use this option if the certificate has been received from the *Certification Authority* in text format.

 —   **Send Certificate File**
 Use this option if the ce rif ic ate has been received from the Certification Authority in file format.

Option. Paste Certificate and Send Certificate

After you have received the certificate from the *Certificate Authority:*

 a   **Copy** (**Ctrl + C**) the certificate information from the *Certificate Authority's* e-mail to the clipboard.

 b   Click **Paste Certificate** to paste the clipboard content into the *Send Certificate* dialog box.

 c   Click the **Send Certificate** button to send the certificate to the *RMX*.

Option. Send Certificate File

After you have received the certificate file from the *Certificate Authority:*

a   Click **Send Certificate File**.

The *Install File* dialog box is displayed.
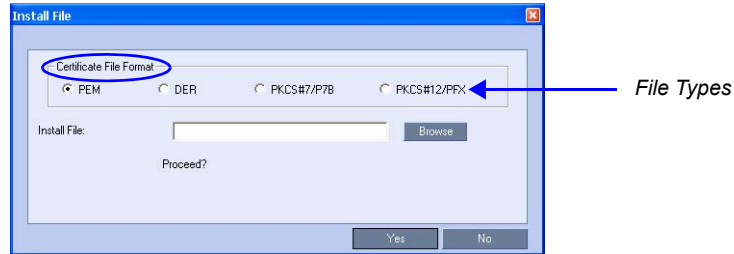
File Types

b   Select the *Certificate File Format*: *PEM, DER, PKCS#7/P7B* or *PKCS#12PFX*.

c   Enter the certificate file name in the *Install File* field or click the **Browse** button.

The *Open* file dialog box is displayed. The files are filtered according to the file type selected in **Step b**.

File Types
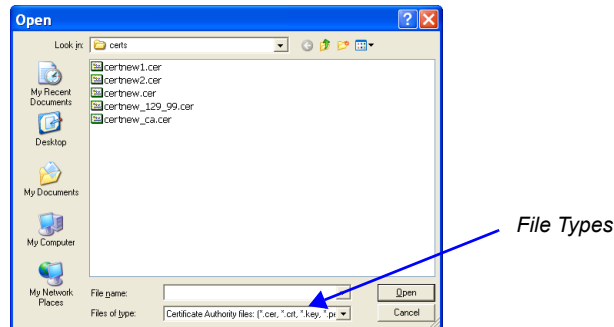
d   Enter the certificate file name in the *File name* field or click to select the certificate file entry in the list.

e   Click the **Open** button.

f   In the *Install File* dialog box, click the **Yes** button to proceed.

The certificate is added to the *Trusted Certificate List* in the *Certification Repository*.

3   If there are additional *Trusted Certificates* to be added to the *Certification Repository,* repeat steps 1 - 2, otherwise click the **Activate Certificate** button to complete *Trusted Certificate / CRL* installation.

Before clicking the **Activate Certificate** button ensure that all *CRL*s have also been added to the *Certification Repository*.

When the **Activate Certificate** button is clicked, all added *Trusted Certificates* and *CRL*s are installed and the *RMX* displays an *RMX Web Client/Manager* disconnection confirmation dialog box.
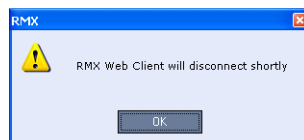
4   Click the **OK** button.

5   Login to the *RMX* to proceed with further management tasks.

Personal Certificates (Management and Signaling Certificates)

Default Management and *Default IP Network Service* certificates can be viewed in the *Personal Certificates* tab.

They are listed alongside the service to which they are attached. By clicking the column headers the *Trusted Certificates* can be sorted by:

- *Network Service*
- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*
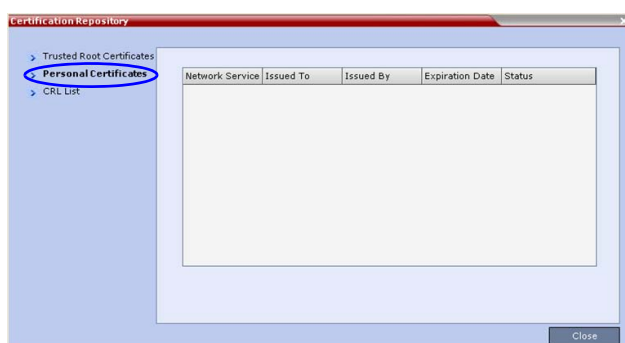
CRL (Certificate Revocation List)

A *CRL* contains a summary of the installed *Certificate Revocation Lists*.

By clicking the column headers the *Certificate Revocation List* can be sorted by:

- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*
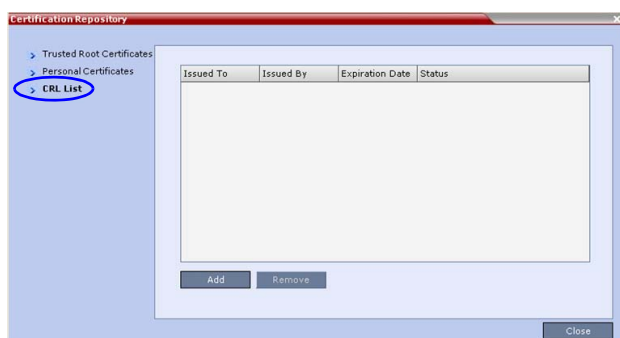
If the *CRL List* is not valid for any reason an *Active Alarm* is created and a message is displayed. The *RMX Web Client/Manager* connection to the RMX is not disabled.

Adding a CRL

To add a CRL to the repository:

Repeat steps 1 - 7 for each *CRL* that is to be added to the *Certification Repository*.

1 In the *CRL List* tab, click the **Add** button.

2 The *Install File* dialog box is displayed.
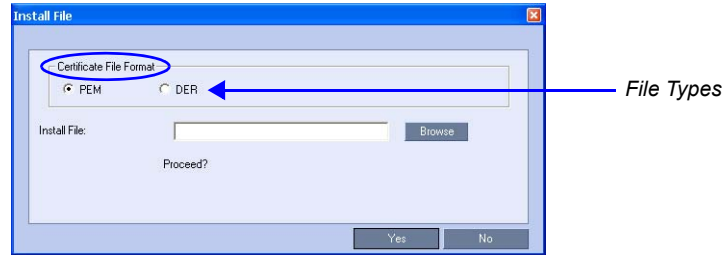
File Types

3 Select the *Certificate File Format*: *PEM* or *DER*.

4 Enter the certificate file name in the *Install File* field or click the **Browse** button.

5 The *Open* file dialog box is displayed. The files are filtered according to the file type selected in **Step b**.

File Types
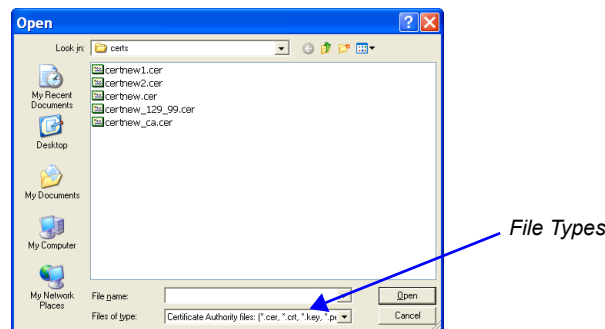
6 Enter the *Certificate* file name in the *File name* field or click to select the certificate file entry in the list.

7 Click the **Open** button.

The certificate is added to the *CRL List* in the *Certification Repository*.

8 If there are additional *CRL*s to be added to the *Certification Repository*, repeat steps 1 - 7, otherwise click the **Activate Certificate** button to complete *CRL / Trusted Certificate* installation.
Before clicking the **Activate Certificate** button ensure that all *Trusted Certificates* have also been added to the *Certification Repository*.

When the **Activate Certificate** button is clicked, all added *Trusted Certificates* and *CRL*s are installed and the *RMX* displays an *RMX Web Client/Manager* disconnection confirmation dialog box.
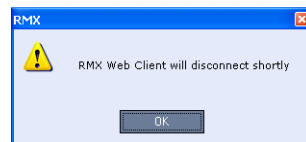
9 Click the **OK** button.

10 Login to the *RMX* to proceed with further management tasks

Removing a CRL

To remove a CRL:

1 In the certificate list, select the *CRL List* to be removed.

2 Click the **Remove** button.

The certificate is removed and the *RMX* displays an *RMX Web Client/Manager* disconnection confirmation dialog box.
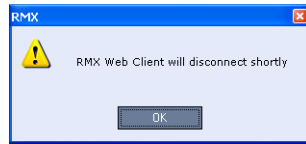
3 Click the **OK** button.

4 Login to the *RMX* to proceed with further management tasks.

Machine Account

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies.

For enhanced security reasons it is necessary for the *RMX* to process user connection requests in the same manner, whether they be from regular users accessing the *RMX* via the *RMX Web Browser / RMX Manager* or from *application-users* representing applications such as *CMA* and *DMA*.

Regular users can connect from any workstation having a valid certificate while application-users representing applications can only connect from specific servers. This policy ensures that a regular user cannot impersonate an *application-user* to gain access to the *RMX* in order to initiate an attack that would result in a *Denial of Service* (*DoS*) to the impersonated application.

A check box, *Associate with a machine* and a new field *FQDN* (*Fully Qualified Domain Name*) have been added to the *User Properties* dialog box.
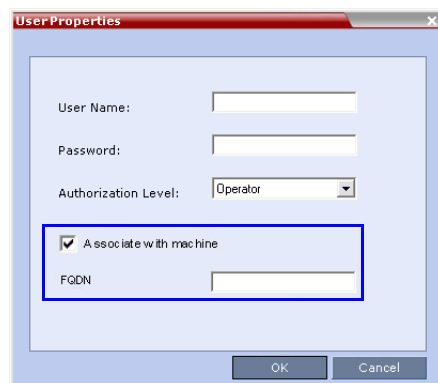
The connection process for an *application-user* connecting to the *RMX* is as follows:

1 The *application-user* sends a connection request, including its *TLS* certificate, to the *RMX*.

2 The *RMX* searches its records to find the *FQDN* that is associated with the *application-user's* name.

3 If the *FQDN* in the received certificate matches that associated with *application-user*, and the password is correct, the connection proceeds.

Guidelines

• *Application-users* are only supported when *TLS* security is enabled and *Request peer certificate* is selected. *TLS* security cannot be disabled until all *application-user* accounts have been deleted from the system.

• For *Secure Communications*, an administrator must set up on the *RMX* system a machine account for the *CMA* system with which it interacts. This machine account must include a fully-qualified domain name (*FQDN*) for the *CMA* system. This *FQDN* field on the *RMX* system is case-sensitive, so it must match the name in the *CMA* certificate (including case) exactly.

• *Application-user* names are the same as regular user names.
Example: the *CMA* application could have an *application-user* name of CMA1.

• The *FQDN* can be used to associate all user types: *Administrator*, *Auditor*, *Operator* with the *FQDN* of a server.

- Multiple *application-users* can be configured the same *FQDN* name if multiple applications are hosted on the same server
- If the system is downgraded the *application-user's FQDN* information is not deleted from the *RMX's* user records.
- A *System Flag,* **PASS_EXP_DAYS_MACHINE,** enables the administrator to change the password expiration period of *application-user's* independently of regular users. The default flag value is 365 days.
- The server hosting an *application-user* whose password is about to expire will receive a login response stating the number of days until the *application-user's* password expires. This is determined by the value of the **PASSWORD_EXPIRATION_WARNING_DAYS** *System Flag*. The earliest warning can be displayed 14 days before the password is are due to expire and the latest warning can be displayed 7 days before passwords are due to expire. An *Active Alarm* is created stating the number of days before the password is due to expire.
- The **MIN_PWD_CHANGE_FREQUENCY_IN_DAYS** *System Flag* does not effect *application-user* accounts. Applications typically manage their own password change frequency.
- If an *application-user* identifies itself with an incorrect *FQDN*, its account will not be locked, however the event is written to the *Auditor Event File.*
- If an *application-user* identifies itself with a correct *FQDN* and an incorrect password, its account will be locked and the event written to the *Auditor Event File.*
- An *application-user* cannot be the last administrator in the system. The last administrator must be regular user.

Monitoring
- An *application-user* and it's connection is represented by a specific icon.

Active Directory
- When working with *Active Directory*, *CMA* and *DMA* cannot be registered within *Active Directory* as regular users. *CMA* and *DMA application-users* must be registered manually.
- The only restriction is that TLS mode is enabled together with client certificate validation.
- If the above configuration are set off it will not be possible to add machine accounts.
- When setting the TLS mode off the system should check the existence of a machine account and block this operation until all machine accounts are removed.

When defining a new user as described in the *RMX 1500/2000/4000 Administrator's Guide*, *"Adding a New User"* on page **13-3**:

1 In the *User Properties* dialog box, select the **Associate with a machine** check box.

2 Enter the *FQDN* of the server that hosts the application who's application-user name is being added. Example: `cma1.polycom.com`

3 Click the **OK** button.

Integration with Microsoft® Active Directory™

It is possible to configure direct interaction between the *RMX* and *Microsoft Active Directory* for *Authentication* and *Authorization* of *Management Network* users.

The following diagram shows a typical user authentication sequence between a *User*, *RMX* and *Active Directory*.
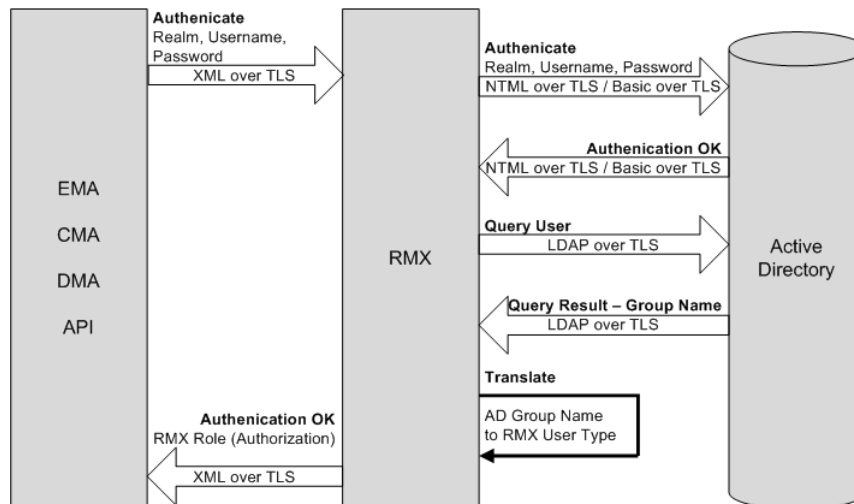
Directory and Database Options

Ultra Secure Mode

Internal RMX database and Active Directory
Authentication is first attempted using the internal *RMX* database. If it is not successful authentication is attempted using the *Active Directory*.

Standard Security Mode

Internal RMX database + External Database
First authentication is via the internal *RMX* database. If it is not successful, authentication is via the *External Database*.

Internal RMX database + External Database + Active Directory

- **Management Logins**

  First authentication is via the internal *RMX* database. If it is not successful, authentication is via the *Active Directory*.

- **Conference Queries** (*Chairperson Password, Numerical ID* etc.)

  First authentication is via the internal *RMX* database. If it is not successful, authentication is via the *External Database*.

Guidelines

- The *RMX* maintains a local record of:
  — *Audit Events* – users that generate these events are marked as being either internal or external.
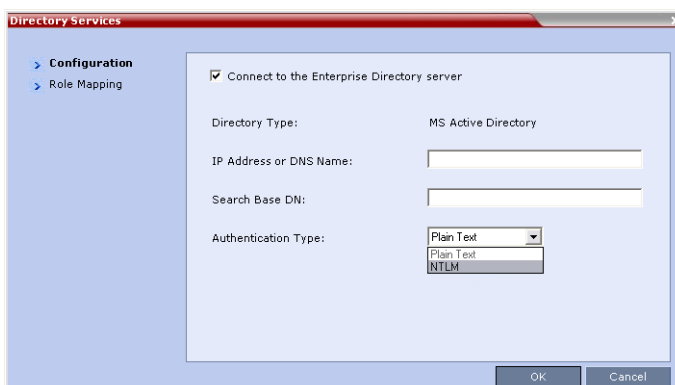
— Successful user logins
— Failed user login attempts

• User passwords and user lockout policy for external users are managed via *Active Directory's* integration with the user's host machine.

• Enabling or disabling *Active Directory* integration does not require a reset.

• In *Standard Security Mode* multiple accounts of all user types are supported. In *Ultra Secure Mode*, enabling *Active Directory* integration is only permitted if the *RMX* only has one local *Administrator User*.

• Multiple *Machine Accounts* with various roles are supported.

• *Microsoft Active Directory* is the only directory service supported.

• *Active Directory* integration is configured as part of the *Management Network*.

• Both *IPv4* and *IPv6* addressing are supported.

• In *Standard Security Mode,* the *Active Directory* can be queried using *Basic* or *NTLM* without *TLS*. In *Ultra Secure Mode TLS* is required.

Enabling Active Directory Integration

To configure Directory Services:

1 On the *RMX* menu, click **Setup > Exchange Integration Configuration**.

The *Directory Services - Configuration* dialog box is displayed.

2 Modify the following fields.

Table 11 Directory Services - Configuration

Field	Description
Connect to the Enterprise Directory Server	Select this check box to enable or disable the *Active Directory* feature.
IP Address or DNS Name	Enter the IP address or DNS name of the Enterprise Directory Server (Active Directory).
Search Base DN	Enter the starting point when searching for *User* and *Group* information in the *Active Directory*. For example if the *Domain Name* is: `mainoffice.bigcorp.com.uk` The entry in this field should be: `CN=Users,DC=mainoffice,DC=bigcorp,DC=come,DC=uk`

Table 11 Directory Services - Configuration (Continued)

Field	Description
Authentication Type	Select the *Authentication Type* from the drop-down menu: • Plain Text • NTLM

3 Click the **Role Mapping** tab.

The *Directory Services - Role Mapping* dialog box is displayed.
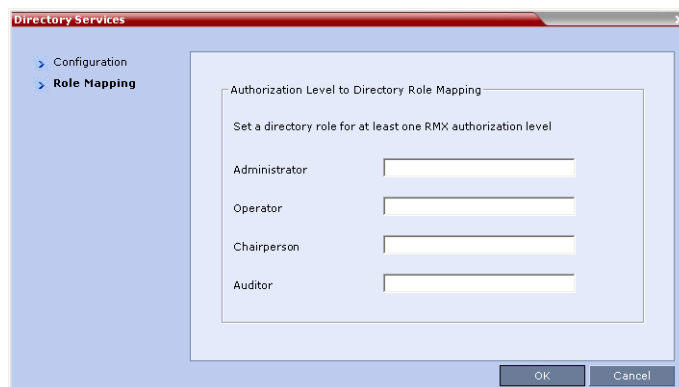
Each of the *RMX* user types: *Administrator*, *Auditor*, *Operator* and *Chairperson* can be mapped to only one *Active Directory Group* or *Role* according to the customer's specific implementation.

— In *Ultra Secure Mode* there are only two user types: *Operator* and *Administrator*.
— An *RMX* user that belongs to multiple *Active Directory Groups* is assigned to the *Group* with the least privileges.

4 Map the *RMX User Types,* to their *Active Directory* roles by modifying the following fields.

Table 12 Directory Services - Role Mapping

Field	Description
Administrator	At least one of these *User Type*s must be mapped to an *Active Directory Role*.
Operator	
Chairperson	
Auditor	

5 Click **OK**.

Multiple Networks

> *SIP* is not supported in *Ultra Secure Mode*.

Media, signaling and Management networks can be physically separated on the RMX system to provide enhanced security. This addresses the requirement in an organization that different groups of participants be supported on different networks. For example, some participants may be internal to the organization while others are external.

Up to eight media and signaling networks can be defined for RMX 4000, or four for RMX 2000 and two for RMX 1500. Multiple *IP Network Services* can be defined, up to two for each media and signaling network connected to the RMX. The networks can be connected to one or several Media cards in the RMX unit.

The *Management Network* is logically and physically separated from the media and signaling networks. There can be one *Management Network* defined per RMX system.

Each conference on the RMX can host participants from the different IP Network networks simultaneously.

Figure 1 on page **1-62** shows the network topology with three different media and signaling networks and one Management network connected to the RMX 4000.
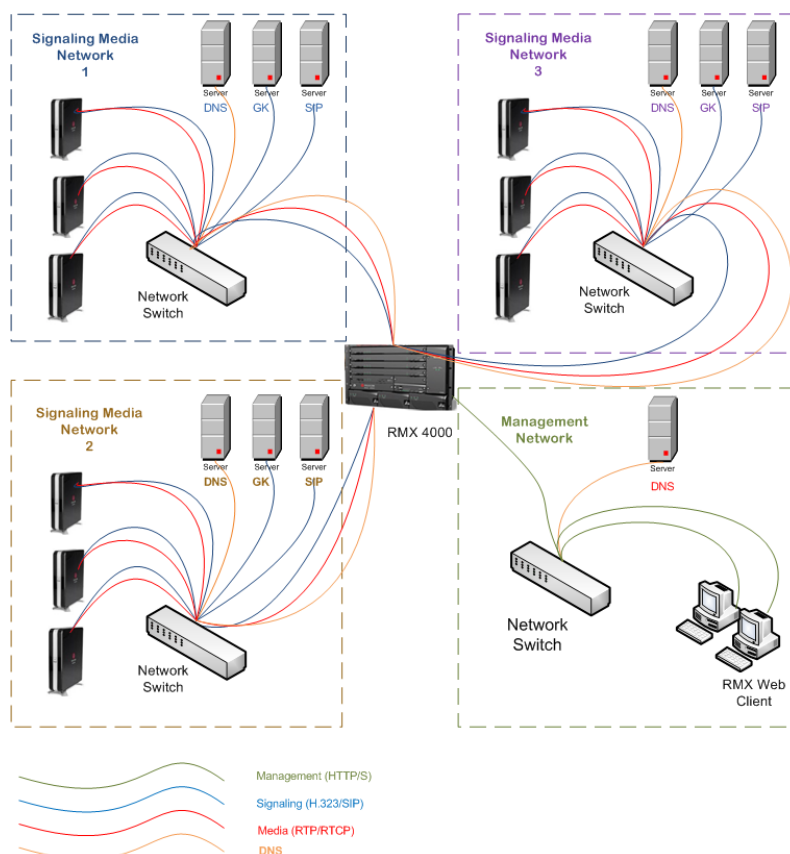
Figure 1   *RMX 4000 - Multiple Network Topology Sample*

Guidelines

- Multiple Services system mode is a purchasable option and it is enabled in the MCU license.
- Multiple Services system mode is enabled when the system configuration flag **MULTIPLE_SERVICES** is added and set to **YES**.

> The *MULTIPLE_SERVICE System Flag* cannot be set to **YES** when *IPv6 Addressing* is enabled.

- This option is supported with MPM+ and MPMx media cards.
- Multiple Network Services are supported in MCUs with at least 1024MB memory only. MCU units with memory of 512MB support only one IP Network Service.
- Multiple Network Services are NOT supported with Microsoft ICE Environments.
- Only IPv4 is supported for the definition of Multiple Network Services.
- Up to two Network Services, one per LAN port, can be associated with each Media card.
- On RMX 2000/4000, RTM ISDN or RTM LAN can be used for Multiple Services configuration. However, if RTM ISDN is installed and used for Multiple Services configuration, only one Network Service can be associated with the media card to which the RTM ISDN card is attached.
- On RMX 1500, when Multiple Network Services option is enabled, the two networks must differ in their subnet masks.
- An IP Network Service can be associated with one or several media cards.
- If more than one card is associated with the same Network Service, the system routes the calls to the appropriate card according to resource availability
- Participants on different networks can connect to the same conference with full audio, video and content capabilities.
- Traffic on one network does not influence or affect the traffic on other networks connected to the same MCU, unless they are connected to the same media card. If one network fails, it will not affect the traffic in the other connected networks, unless they are connected to the same media card and the card fails.
- Maximum number of services that can be defined per RMX platform:

Table 13   Maximum Number of IP Network Service per RMX Platform

RMX Platform	IP Network Services	Management Services
RMX 1500	Up to 2	1
RMX 2000	Up to 2 (combination of RTM ISDN and/or RTM LAN) or Up to 4 (using 2 RTM LAN cards, less when using up to 2 RTM ISDN cards)	1
RMX 4000	Up to 4 (Up to 2 RTM ISDN cards and the remaining RTM LAN cards) Up to 8 (using 4 RTM LAN, less when using up to 2 RTM ISDN cards)	1

- Only one DNS server can be defined for the entire configuration. It is recommended to define it in one of the IP Network Services (signaling) and not the Management Network to enable dialing in/out using names.
    — In the Network Services that do not include the DNS, use the IP addresses of the various devices to define them in the Network Services.
- Participants are associated with a Network Service and use it resources as follows:
    — Dial-in participants - according to the network used to place the call and connect to the RMX.
    — Dial-out participant - according to the Network Service selected during the participant properties definition by the RMX administrator or during conference definition, according to the Network Service selected as default by the RMX administrator.

Resource Allocation and Capacity

The *Video/Voice Port Configuration* and the *Resolution Configuration* settings are configured per MCU and affect the resource capacity of the MCU. They are reflected in the port gauges displayed on the RMX management application's main screen. In *Multiple Networks* mode, the overall resources as configured in the *Video/Voice Port Configuration* are divided between the Network Services. However, the port gauges do not reflect the resource availability per Network Service.

Fixed and Flexible Resource Allocation Mode

On RMX 2000/4000 resources are divided between services according to the number of media cards associated with each service and the card assembly type (for example, MPM+40 vs. MPM+80). If two identical media cards are installed in the system and each card is assigned to a different Network Service, the resources are split between the services.

If two cards are installed but each card is of different assembly type, the resources are allocated according to the card capacity ratio. For example, in a system with one MPM+40 and one MPM+80, the capacity ratio is 1 to 2, therefore a third of the resources will be assigned to the network service associated with MPM+40 and two thirds will be assigned to the Network Service associated with MPM+80.

On RMX 1500 and RMX 2000/4000 with two *Network Services* associated with one media card, the resources of the two Network Services associated with one media card are not split between the network services. In such a case, resources are used per their availability by both Network Services equally.

On RMX 2000, if RTM ISDN is installed and used for Multiple Services configuration, only one Network Service can be defined per media card.

In *Fixed Resource Allocation Mode* if the resources cannot be divided into whole numbers, they will be rounded up to the nearest whole number, assigning that resource to the *Network Service* with the higher capacity (i.e. more media cards or media cards with higher capacity due to a different card assembly).

First Time Installation and Configuration

First Time Installation and Configuration of the RMX 1500/2000/4000 consists of the following procedures:

1   **Preparations**:
    — Gather Network Equipment and Address Information - get the information needed for integrating the RMX into the local network for each of the networks that will be connected to the RMX unit. For a list of required

address, see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "Procedure 2: Gather Network Equipment and Address Information"* on page **1-11**.

2   **Hardware Installation and Setup**

— Mount the RMX in a rack. For more details see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "Procedure 1: Hardware Installation and Setup"* on page **1-3**.

— Connect the necessary cables. For details, see *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "Cabling the RMX 2000/4000"* on page **1-6**.

3   **First Entry Power-up and Configuration**

— Power up the RMX. For more details see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "First-time Power-up and Connection to MCU"* on page **1-15**.

— Register the RMX. For more details see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "Product Registration"* on page **1-14**.

— Connect to the RMX. For more details see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "First-time Power-up and Connection to MCU"* on page **1-15**.

— Configure the *Default IP Network Service* using the information for one of the networks connected a media card installed in the system. For more details see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "Modifying the Signaling Network Service and ISDN/PSTN Network Service Settings"* on page **1-22**.

— **Optional.** Configure the *ISDN/PSTN Network Service.* For more details see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments.*

4   Modify the required System Flag to enable Multiple Services and reset the MCU.

5   Add the required IP Network Services to accommodate the networks connected to the RMX unit.

6   Select a Network Service to act as default for dial out and gateway calls for which the Network Service was not selected.

7   Place several calls and run conferences to ensure that the system is configured correctly.

Upgrading to Version 7.5.0.J and Multiple Services

1   Gather Network Equipment and Address Information for each of the networks that will be connected to the RMX unit. For a list of required address, see *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments,"IP Network Services Required Information"* on page **1-11**.

2   Upgrade the software version to Version 7.5.0.J and install the activation key that contains the Multiple Services license as described in *"Upgrade Paths to Version 7.5.0.J"* on page **23**.

3   Place several calls and run conferences to ensure that the system upgrade was completed successfully.

4   Modify the required System Flag to enable Multiple Services, DO NOT reset the MCU yet.

5   Connect the additional network cables to the RMX and change existing connections to match the required configuration as described in the *"RMX Hardware Installation"* on page **67**.

At this point, the Management Network can be modified to match the required local network settings.

> If the RMX 2000 you are upgrading does not include RTM ISDN or RTM LAN cards, you must install at least one RTM LAN card to enable the definition of multiple Network Services. If no RTM ISDN or RTM LAN cards are installed, the RMX 2000 works in a single Network Service mode and an alarm is issued by the system. For more details about the installation of RTM LAN cards, see the *RMX 2000 Hardware Guide*.

6   Reset the MCU.

7   Connect to the MCU and Add the required IP Network Services to accommodate the networks connected to the RMX unit.

8   Select a Network Service to act as default for dial out and gateway calls for which the Network Service was not selected.

9   Place several calls and run conferences to ensure that the system is configured correctly.

Gather Network Equipment and Address Information - IP Network Services Required Information

It is important that before connecting multiple networks and implementing Multiple Services in the RMX, that you obtain the information needed to complete the **IP Network Service** configuration for each connected network from your network administrator.

Table 14   Network Equipment and Address Information per IP Network Service

Parameter	Local Network Settings	Note
Signaling Host IP address		
Media Board IP address (MPM 1)		
Media Board IP address (MPM 2) **RMX 2000/4000 only**		If more than one media card is associated with this Network Service
Media Board IP address (MPM 3) **RMX 4000 only**		If more than one media card is associated with this Network Service
Media Board IP address (MPM 4) **RMX 4000 only**		If more than one media card is associated with this Network Service
Gatekeeper IP address (optional)		
DNS IP address (optional)		Only one DNS can be defined for the entire Network topology
SIP Server IP address (optional)		

RMX Hardware Installation

> When connecting the LAN cables of the various networks to the RMX it is recommended to use a color system to differentiate between the networks, for example, using colored cables.

RMX 4000 Multiple Services Configuration

Connecting the cables to the RTM IP 4000:

The following cables are connected to the RTM IP on the rear panel of the RMX 4000:
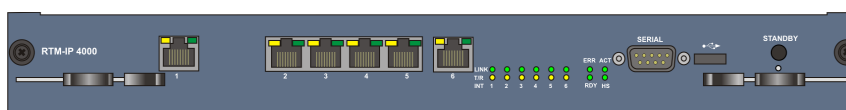
Table 15   *LAN Connections to the RTM IP*

RTM IP Port	Description
LAN 1	Modem
LAN 2	Management
LAN 3	–
LAN 4	–
LAN 5	–
LAN 6	Shelf Management

Connecting the cables to the RTM LAN:

Table 16   *LAN Connections to the RTM LAN*

RTM LAN Port	Description
LAN 1	Signaling and Media - additional (second) Network Service
LAN 2	Signaling and Media - existing (first) Network Service

Figure 2 shows the cables connected to the RMX 4000 rear panel, when one RTM ISDN and three RTM LAN cards are installed providing IP and ISDN connectivity. The RTM ISDN card can be used for both ISDN and IP calls and only one IP network Service is associated with each RTM LAN card.
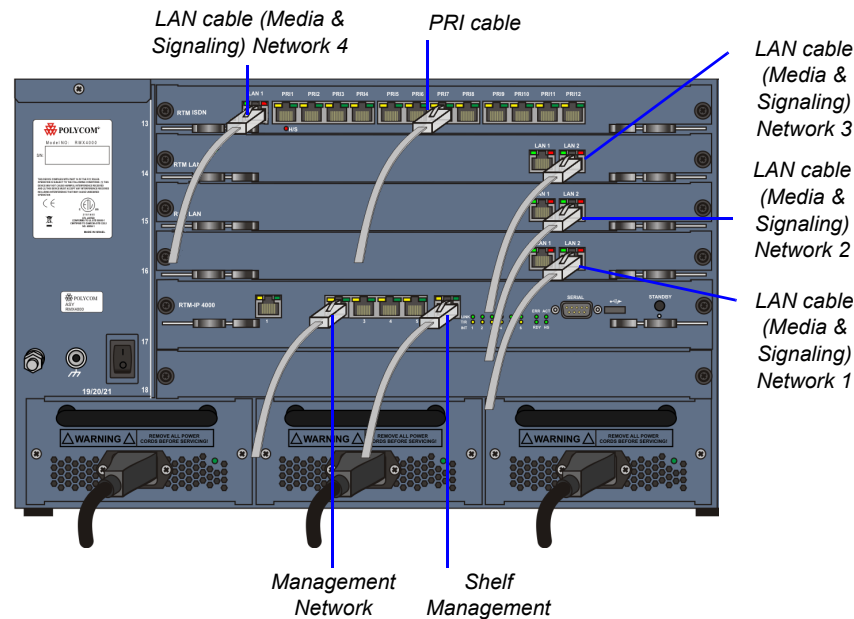
Figure 2   *RMX 4000 Rear Panel with LAN and PRI cables*

In this case, up to four different IP Network Services can be defined - one for each RTM LAN/RTM ISDN cards installed in the system.

If two LAN ports per each installed RTM LAN card are used, up to three additional Network Services can be defined, bringing it to a total of up to 7 IP Network Services.

Several cards can be assigned to the same IP Network Service. The definition of the network services attached to the RMX unit and which cards are assigned to each network service is defined in the IP Network Service.

RMX 2000 Multiple Services Configuration

Connecting the cables to the RTM IP:
The following cables are connected to the RTM IP on the rear panel of the RMX2000:
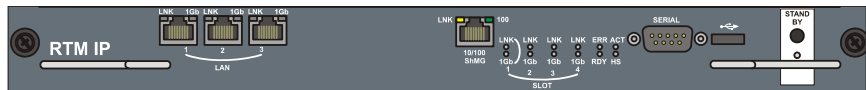
Table 17   *LAN Connections to the RTM IP*

RTM IP Port	Description
LAN 1	–
LAN 2	Management
LAN 3	Modem

Connecting the cables to the RTM LAN:

> If RTM LAN or RTM ISDN cards are not installed on the RMX, they must be installed before connecting the additional network cables for media and signaling.

Table 18   *LAN Connections to the RTM LAN*

RTM IP Port	Description
LAN 1	Signaling and Media - second Network Service (optional)
LAN 2	Signaling and Media - first Network Service (optional)

If one LAN port per RTM ISDN/ RTM LAN card is used, up to two different IP Network Services can be defined - one for each installed RTM LAN/RTM ISDN cards.

If two LAN ports per each installed RTM LAN card are used, up to four Network Services can be defined.

Figure 3 shows the cables connected to the RMX 2000 rear panel, when two RTM LAN cards are installed providing IP connectivity. In this case, only one IP network Service can be associated with each RTM LAN card.
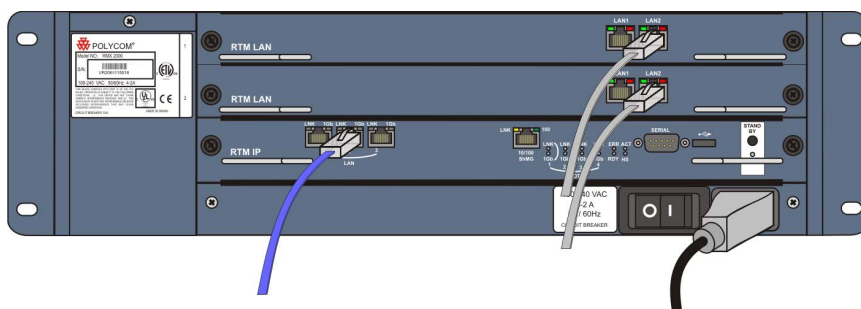
Figure 3   *RMX 2000 Rear Panel with RTM LAN Cables*

RMX 1500 Multiple Services Configuration

Connecting the cables to the RTM IP 1500:
The following cables are connected to the RTM IP on the rear panel of the RMX 1500:
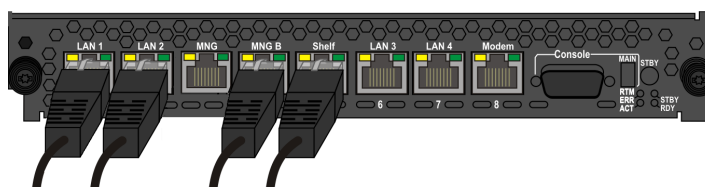
Table 19   *LAN Connections to the RTM IP*

RTM IP Port	Description
LAN 1	Media and signaling - additional (second) Network Service
LAN 2	Media and signaling - existing (first) Network Service

Table 19   *LAN Connections to the RTM IP*

RTM IP Port	Description
MNG	–
MNG B	Management
Shelf	Shelf Management
LAN 3	–
LAN 4	–
Modem	Modem

RMX Configuration

Once the network cables are connected to the RMX unit, you can modify the default IP Network Service and add additional Network Services.

System Flags and License Settings

The **MULTIPLE_SERVICES** System Flag determines whether the Multiple Services option will be activated once the appropriate license is installed. Possible Values: **YES / NO** Default: **NO**

This flag must be manually added to the system configuration and set to YES to enable this option. For more information see the RMX 1500/2000/4000 Administrator's Guide, "*Manually Adding and Deleting System Flags"* on page **19-21**.

> If the MULTIPLE_SERVICES System Flag is set to YES and no RTM ISDN or RTM LAN card is installed in the RMX 2000, an Active Alarm is displayed.

> If the values or either of the MULTIPLE_SERVICES or V35_ULTRA_SECURED_SUPPORT *System Flags* are changed from YES to NO, the defined *IP Network Services* are not displayed in the *IP Network Services* list pane: they are, however, saved in the system.
> If either of the flag values are changed back to YES, the saved defined *IP Network Services* will be displayed.

IP Network Service Definition
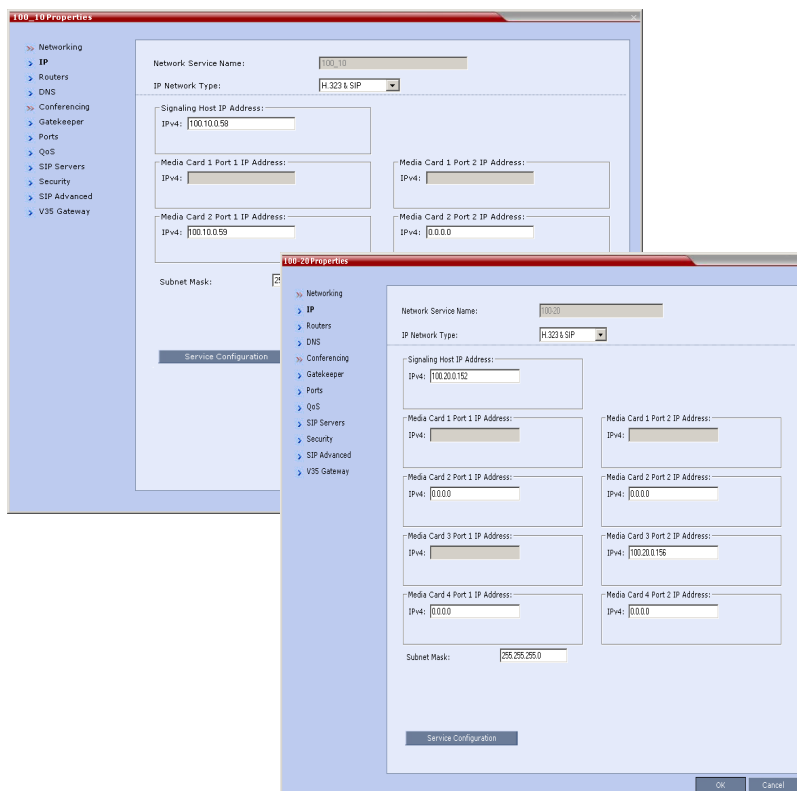
Use this procedure to define Network Services in addition to the Network Service already defined during first entry installation and configuration. Each of the defined Network Service can be associated with one or more media cards installed in the system (depending on the system type).

Once a media card is associated with a Network Service it **cannot be** associated with another network service.

To add new/additional Network Services:

1   In the *Device Management* pane, click **IP Network Services** (⊕).

2   In the *Network Services* list toolbar, click the **Add Network Service** button.

The *New IP Service - Networking IP* dialog box opens.

3   Define the following fields:

Table 20   Default IP Network Service – IP

Field	Description
Network Service Name	Enter the IP Network Service name. **Note:** This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.
IP Network Type	Select the IP Network environment. You can select: • **H.323:** For an H.323-only Network Service. • **SIP:** For a SIP-only Network Service. • **H.323 & SIP:** For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	Enter the address to be used by IP endpoints when dialing into the MCU using this Network Service. Dial out calls of participants to whom this network service will be assigned are initiated from this address. This address is used to register the RMX with a Gatekeeper or a SIP Proxy server residing on this network.

Table 20 *Default IP Network Service – IP (Continued)*

Field	Description
Media Card 1 Port 1 IP Address *Media Card 1Port 2 IP Address 2*	If only one network is connected to this media card, it is enough to assign one media card to this Network Service. In such a case, enter one IP address for the media card according to the LAN Port used for the connection. If each of the LAN ports on one media card is used with two different networks, each port is assigned to its own Network Service. In such a case, enter the IP address of the port to be assigned to this Network Service. A LAN port that is already assigned to a different Network Service, displays the IP Address of the assigned port and it cannot be assigned to this Network Service (it is disabled).
Media Card 2 Port 1 IP Address (RMX 2000/4000) *Media Card 2 Port 2 IP Address (RMX 2000/4000)* *Media Card 3 Port 1 IP Address (RMX 4000)* *Media Card 3 Port 2 IP Address (RMX 4000)* *Media Card 4 Port 1 IP Address (RMX 4000)* *Media Card 4 Port 2 IP Address (RMX 4000)*	If only one network is connected to this media card, it is enough to assign one media card to this Network Service. In such a case, enter one IP address for the media card according to the LAN Port used for the connection, as provided by the network administrator. If each of the LAN ports on one media card is used with two different networks, each port is assigned to its own Network Service. In such a case, enter the IP address of the port to be assigned to this Network Service. **Notes:** • LAN Ports/Media cards that are already associated with another Network Service cannot be associated with this Network Service. • You can define a Network Service without assigning media cards to it. • To change the assignment of a card from one service to another, the card must first be removed from the service to which it is assigned prior to its assignment to another service. **RMX 2000:** If one card was already assigned to another service, only one additional card can be assigned to this service. **RMX 4000:** Depending on the number of media cards installed in the system, you can assign up to 4 media cards to this network service provided that they are not assigned to any other Network Service.
Subnet Mask	Enter the subnet mask of the MCU in that network service. Default value: 255.255.255.0.

4 **Optional.** Some system flags can be defined per Network Service, depending on the network environment.
To modify these flags, click the **Service Configuration** button.

The *Service Configuration* dialog box opens.
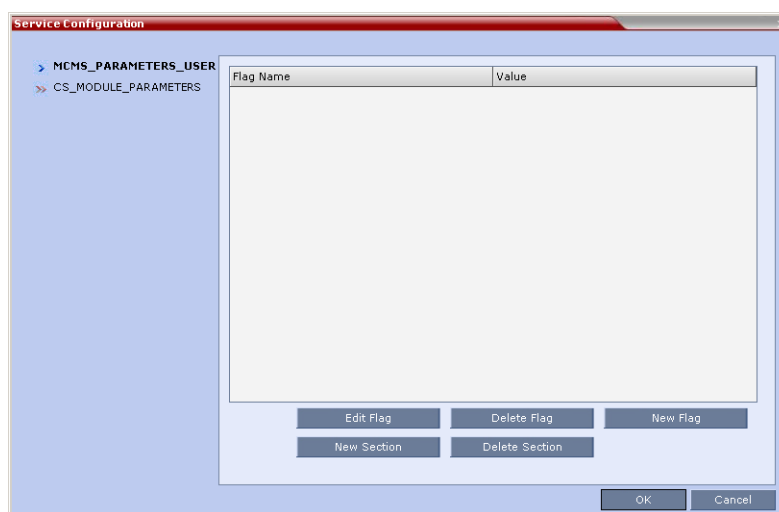
All the flags must be manually added to this dialog box. For a detailed description of the flags and how to add them, see the *RMX 1500/2000/4000 Administrator's Guide, "Manually Adding and Deleting System Flags"* on page **19-21**.

Flags defined per Network Service override their general definition in the System Configuration.

The following flags can be defined per service:

— ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF
— SIP_ENABLE_FECC
— ENABLE_H239
— SIP_ENABLE_FECC
— ENABLE_CLOSED_CAPTION
— ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF
— NUMERIC_CONF_ID_LEN
— NUMERIC_CONF_ID_MIN_LEN
— NUMERIC_CONF_ID_MAX_LEN
— ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD
— MAX_CP_RESOLUTION
— QOS_IP_AUDIO
— QOS_IP_VIDEO
— ENABLE_CISCO_GK
— SIP_FREE_VIDEO_RESOURCES
— FORCE_CIF_PORT_ALLOCATION
— MS_ENVIRONMENT
— SIP_FAST_UPDATE_INTERVAL_ENV
— SIP_FAST_UPDATE_INTERVAL_EP
— H263_ANNEX_T
— H239_FORCE_CAPABILITIES
— MIX_LINK_ENVIRONMENT
— IP_LINK_ENVIRONMENT
— FORCE_STATIC_MB_ENCODING
— FORCE_RESOLUTION
— SEND_WIDE_RES_TO_IP
— DISABLE_WIDE_RES_TO_SIP_DIAL_OUT

73

— SEND_SIP_BUSY_UPONRESOURCE_THRESHOLD

5   Click the **Routers** tab.

6   Define the routers used in this network and that are other than the routers defined in the Management Network. The field definitions of the *Routers* tab are the same as for the *Default Management Network.* For more information see the RMX 1500/2000/4000 Administrator's Guide, "*Click the Routers tab."* on page **14-16**.

7   Click the **DNS** tab.
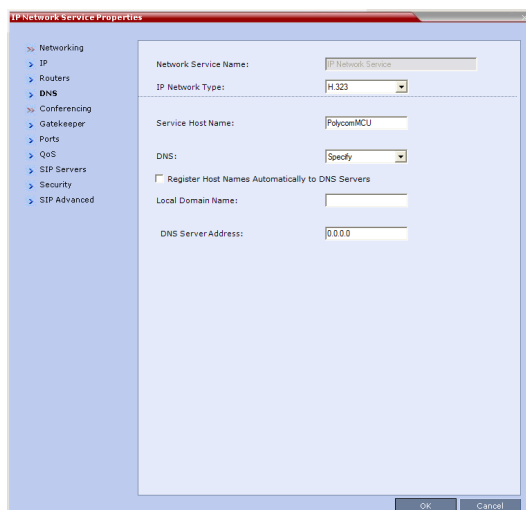
8   Modify the following fields:

Table 21   *Default Management Network Service – DNS*

Field	Description
Service Host Name	Enter the host name of this network Service. Each Network Service must have a unique Host Name otherwise an error message is displayed.
DNS	Select: • **Off** – if no DNS server is used in this network. • **Specify** – to enter the IP address of the DNS server used by this network service. **Notes:** • The IP address field is enabled only if **Specify** is selected. • Only one DNS can be define for the entire topology (that is, only one Network Service can include the DNS definition).
Register Host Names Automatically to DNS Servers	Select this option to automatically register this Network Service Signaling Host with the DNS server.
Local Domain Name	Enter the name of the domain for this network service.
DNS Server Address	Enter the static IP address of the DNS server that is part of this network.

9 Click the **Gatekeeper** tab.

10 Define the *Primary* and *Alternate Gatekeepers* and at least one **Alias** for this network Service. The field definitions of the *Gatekeeper* tab are the same as for the *Default IP Network Service*. For more information see the RMX 1500/2000/4000 Administrator's Guide, "*Click the Gatekeeper tab.*" on page **14-17**.

> In *Multiple Services* mode, an Alias must be defined for the specified gatekeeper.

11 **Optional.** Click the **Ports** tab.

Settings in the *Ports* tab allow specific ports in the firewall to be allocated to multimedia conference calls. If required, defined the ports to be used multimedia conference calls handled by this Network Service. The field definitions of the *Ports* tab are the same as for the *Default IP Network Service*.

For more information see the RMX 1500/2000/4000 Administrator's Guide, "*Click the Ports tab.*" on page **14-20**.

12 If required, click the **QoS** tab.

RMX's implementation of *QoS* is defined per Network Service, not per endpoint.

> The routers must support QoS in order for IP packets to get higher priority.

The field definitions of the *QoS* tab are the same as for the *Default IP Network Service*. For more information see the RMX 1500/2000/4000 Administrator's Guide, "*If required, click the QoS tab.*" on page **14-22**.

13 Click the **Security** tab.

The field definitions of the *Security* tab are the same as for the *Default IP Network Service*. For more information see the RMX 1500/2000/4000 Administrator's Guide, "*Click the Security tab.*" on page **14-28**.

14 Click the **OK** button.
The new Network Service is added to the *IP Network Services* list pane.

Setting a Network Service as Default

The default Network Service is used when no Network Service is selected for the following:

* Dial out participants
* Reserving resources for participants when starting an ongoing conference
* Gateway calls

In addition, the Signaling Host IP address and the MCU Prefix in GK displayed on the RMX Web Client main screen are taken from the default H.323 Network Service.

One IP Network Service can be defined as default for H.323 connections and another Network Service as default for SIP connections. If the IP Network Service supports both H.323 and SIP connections, you can set the same Network Service as default for both H.323 and SIP, or for H.323-only or for SIP-only.

To designate an IP Network Service as the default IP Network Service:

1 In the *Device Management* pane, click **IP Network Services** ( ).

2 In the *Network Services* list pane right-click the IP Network Service to be set as the default, and then click **Set As H.323 Default,** or **Set As SIP Default**.

The next time you access this menu, a check mark is added next to the network service type to indicate its selection as default.

To set this IP Network Service for both H.323 and SIP connections, repeat step 2 and select the option you need.

The following icons are used to indicate the default IP Network Service type:

Table 1-1: Default IP Network Service Icons

Icon	Description
	This Network Service supports both SIP and H.323 connections and is designated as default for both SIP and H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for SIP connections.
	This Network Service supports only H.323 connections and is set as default for H.323 connections.
	This Network Service supports only SIP connections and is set as default for SIP connections.

Ethernet Settings

The RMX 2000 is set to automatically identify the speed and transmit/receive mode of each LAN ports located on the RTM LAN or RTM ISDN cards that are added to the system. These port settings can be manually configured if the specific switch requires it, via the **Ethernet Settings** as for RMX 1500/4000. For more details, see RMX 1500/2000/4000 Administrator's Guide, "*Ethernet Settings"* on page **14-30**.

> **RMX 1500:** The *Port* numbers displayed in the dialog box do not reflect the physical *Port* numbers as labeled on the *RMX 1500* MCU.

Signaling Host IP Address and MCU Prefix in GK Indications

The RMX Web Client displays the *Signaling Host IP Address* and *MCU Prefix in GK* parameters as defined in the **Default H.323 Network Servic**e.
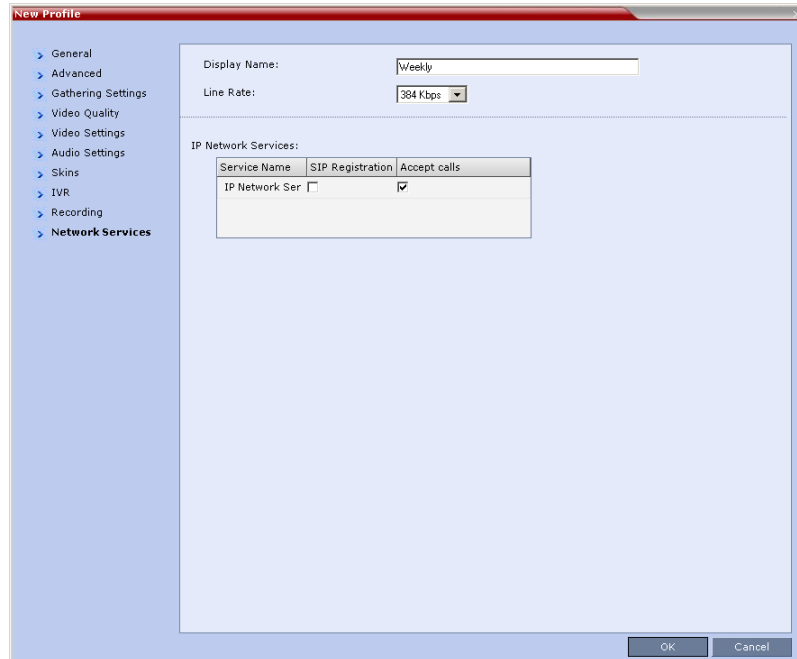
Video/Voice Port Configuration and Resolution Configuration

These configurations are set for the system and are applied to all the Network Services.

Conference Profile

Registration of conferencing entities such as ongoing conferences, Meeting Rooms, Entry Queues, SIP Factories and Gateway Sessions with SIP servers is done per conferencing entity. This allows better control on the number of entities that register with each SIP server by selecting for each of the conferencing entities whether it will register with the SIP server.

The registration is defined in the *Conference Profile - Network Services* tab.
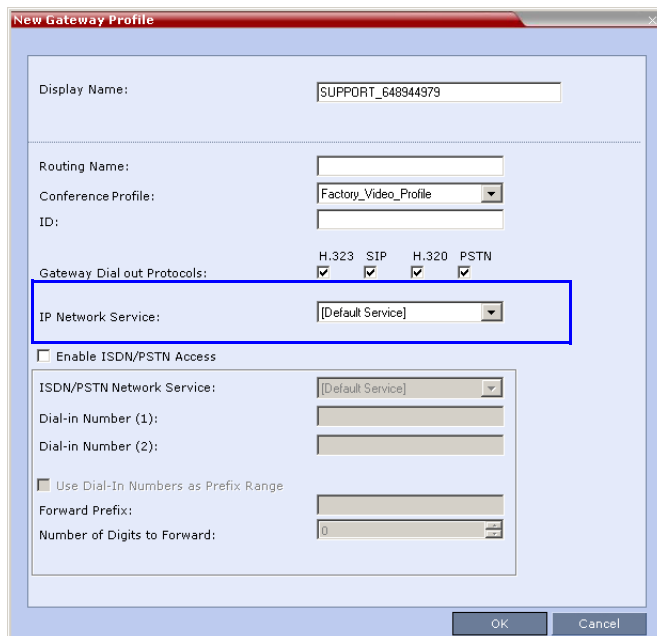
In the *IP Network Services* table, the system lists all the defined Network Services (one or several depending on the system configuration).

- To register the conferencing entity to which this profile is assigned to a Network Service, in the *Registration* column click the check box of that Network Service.

- You can also prevent dial in participants from connecting to that conferencing entities when connecting via a Network Service.
  In the *Accept Calls* column, clear the check box of the Network Service from which calls cannot connect to the conference.

Gateway Profiles

To enable the RMX to call the destination endpoint/MCU via IP connection, the Network Service for the call must be selected in the Gateway Profile dialog box.

The Network Service set as default is used if no other Network Service is selected.

If the same Network Service is used for H.323 and SIP calls, the *Network Service Environment* must include both **H.323** and **SIP** settings.

Hardware Monitor

The Hardware Monitor pane includes the status of the LAN ports on the RTM LAN cards.

Signaling Monitor

The Signaling Monitor pane includes the list of the IP Network Services defined in the system (up to two in RMX 1500/2000 and up to four in RMX 4000). Double-clicking a Network Service, displays it properties and status.

Signaling Monitor (4)			
Name	IP Address	Router	Subnet Mask
IP Network Servic	200.10.0.152	200.10.0.1	255.255.255.0
IP2	100.10.0.150	100.10.0.1	255.255.255.0
100-30	100.30.0.152	100.30.0.1	255.255.255.0
100-20	100.20.0.152	100.20.0.1	255.255.255.0

Conferencing
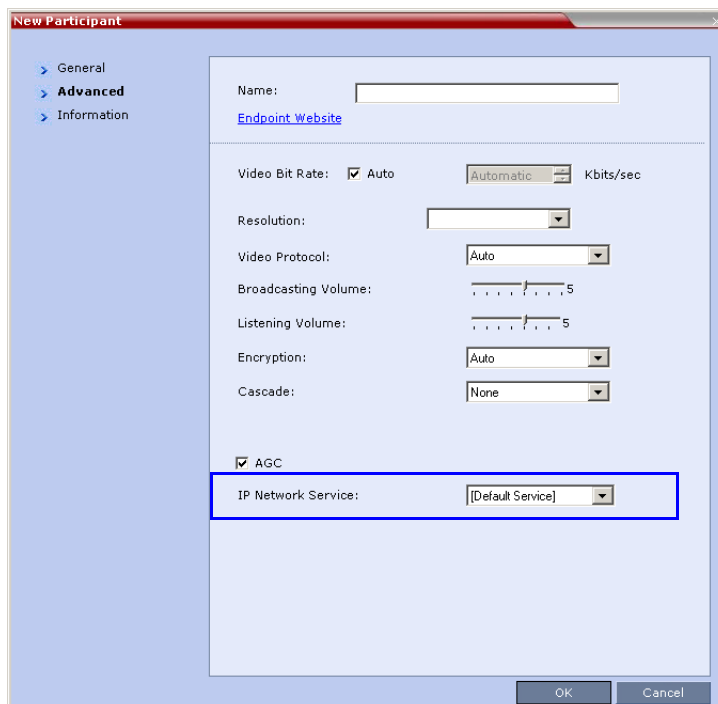
Each conference on the RMX can host participants from the different IP Network networks simultaneously.

Defining Dial Out Participants

When defining dial out participants, you can select the Network Service to place the call according to the network to which the endpoint pertains. If the endpoint is located on a network other than the selected network, the participant will not be able to connect.

If no Network is selected, the system uses the IP Network Service selected for reserving the conference resources, and if none is set for the conference it uses the Network Service set as default.

The IP Network Service is selected in the *New Participant - Advanced* dialog box.
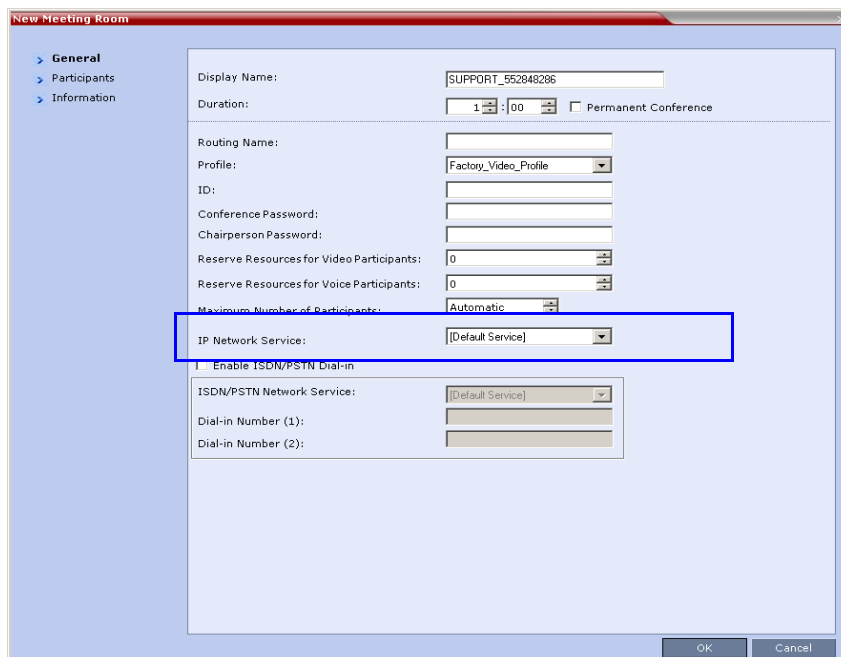
Reserving Video Resources for a Conference

When defining a new ongoing conference or a conference reservation, you can select the Network Service that will be used to reserve the required resources. If no Network Service is selected, the default Network Service is used. Therefore, make sure that not all conferences are reserving resources from the same Network Service, otherwise you may run out of resources for that Network Service.

The IP Network Service is selected in the *New Conference/New Meeting Room/New Reservation - General* dialog box.

Monitoring Conferences

The *Conference Properties - Network Services* dialog box shows for each Network Service with which Network Service's SIP proxy the conference should be registered and if the dial in call will be connected to the conference.

In the *Participant* pane, a new column - *Service Name* was added, indicating the name of Network Service used for the participant's connection.

Resource Report

The *Resource Report* displays the resource usage in total and per Network Service in a table format. The Resources per Service table provides the actual information on resource usage and availability per network Service and provides an accurate snapshot of resources usage in the system.

You can select the graph to display: select either **Totals** (default) or the Network Service.
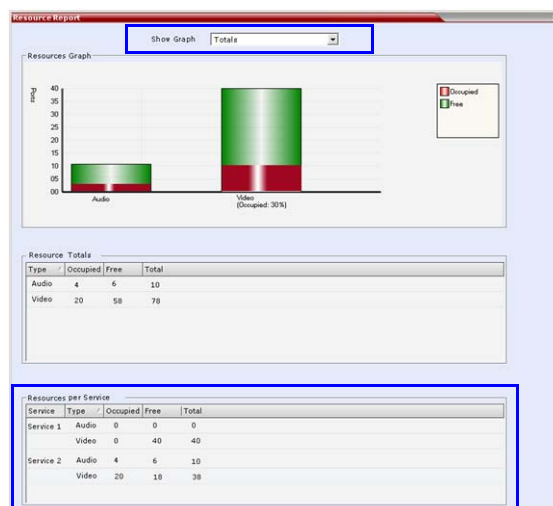
Port Gauge Indications

The port Gauges displays the total resource usage for the RMX and not per Network Service. Therefore, it may not be an accurate representation of the availability of resources for conferencing, as one Network Service may run out of available resources while another Network Service may have all of it resources available. In such a case, the port gauges may show that half of the system resources are available for conferencing, while calls via the Network Service with no available resources will fail to connect.

Antivirus

McAfee® SDK Antivirus, included in this version, can be enabled/disabled, updated and scanning times can be set and scheduled.

The *McAfee® SDK Antivirus* application scans the following types of files:

- All *files* that are sent and loaded to the *RMX*
- All RMX versions
- *IVR* files
- *TLS* certificates
- *Restore* and *Backup* configuration files

Guidelines

- *McAfee® SDK Antivirus* is supported in *Ultra Secure Mode*.
- *Audit* files entries resulting from *Antivirus* scans are time stamped in *GMT*.
- *Zip* files cannot be un compressed.
- *RMX 2000's* with *512Mb Control Units* are not supported.

Scheduling
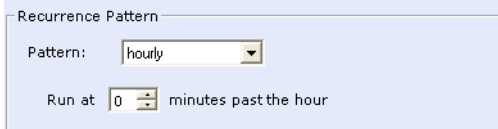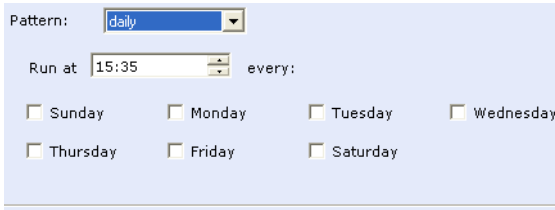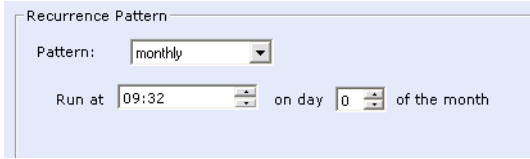
The *McAfee® SDK Antivirus* application must be enabled and scheduled by an administrator or a user with administrator permissions.

1 To enable/disable the Antivirus Application/Scan:

2 In the *Setup* menu, click **Antivirus** to open the *Antivirus* dialog box.

3 Enable/Disable the Antivirus application/scan by selecting the **Anti Virus Scan** check box. When enabled and a scan is not scheduled, the system will initiate based on the default setting.
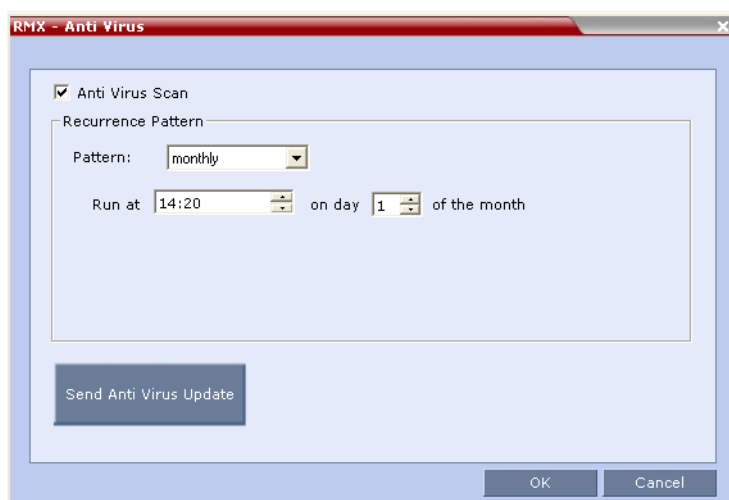
4 When enabled, adjust the antivirus scheduling by modifying the fields as described in Table 2.

Table 2   *Antivirus – Scheduling*

Field		Description
Recurrence Pattern	Hourly	If *hourly* is selected, then choose the *minutes past the hour* to run the antivirus application.
Recurrence Pattern (cont.)	Daily	If *Daily* is selected, choose the day of the week to run the antivirus application.
	Monthly	Select the day (1-31)of the month to run the antivirus application.

Update the Antivirus DAT file

For more information see "Antivirus Updates" on page **1-84**.

5 Click **Send Aniti Virus Update** to open the *Install Software* dialog box.
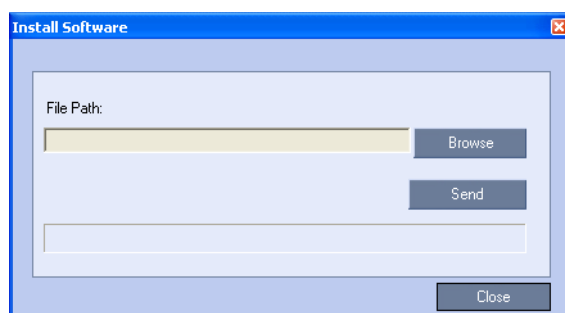
6 Click **Browse** and determine the file location and then select the file.

> The McAffee file is converted automatically to a TAR file with a .tgz file extension.

7 Click **Send** to install the file.When uploaded, the DAT file is checked and verified on the RMX.

a If the file is found to be invalid, an error message "*The DAT file is invalid*" appears on screen.

> **b** Reload the DAT file.

8 Click **Close**.

> - Schedule anti-virus scans in accordance with your site policies.
> - Anti-virus scans impose a significant burden on the system that could impact system performance. Schedule system scans for times when the system is in maintenance mode or when little or no conferencing activity is anticipated.

Scan Results

If a virus is detected an *Active Alarm* is triggered: "*Antivirus detected: <text from Antivirus>*".

Reset the *RMX* to remove or cancel the *Active Alarm*. When a new scan is initiated and the antivirus warning has not been removed the *Active Alarm* is reactivated.

In the *Faults* list when the *Antivirus* scan activates the following message appears: "*Antivirus scan running*".
Upon completion of the scan the *Fault* list displays a follow-up message: "*Antivirus scan completed*".

Antivirus Updates

The administrator must manually update the .dat file, containing signature file updates, of the *McAfee® SDK Antivirus* application. This *DAT* file must retrieved from the official McAfee® web site at the following web address:
http://update.nai.com/Products/CommonUpdater

Locate the 75+ Mb file: **avvdat-xxxx.zip**
For example: **avvdat-6194.zip**

Index of /Products/CommonUpdater

Name	Last modified	Size	Description
Parent Directory		–	
current/	03-Sep-2010 15:59	–	
61596160avv.gem	11-Dec-2010 11:11	79K	
61856186avv.gem	11-Dec-2010 11:11	29K	
61866187avv.gem	11-Dec-2010 11:11	170K	
61876188avv.gem	11-Dec-2010 11:11	51K	
61886189avv.gem	11-Dec-2010 11:11	57K	
61896190avv.gem	11-Dec-2010 11:11	65K	
61906191avv.gem	11-Dec-2010 11:11	43K	
61916192avv.gem	11-Dec-2010 11:11	108K	
61926193avv.gem	11-Dec-2010 11:11	112K	
61936194avv.gem	11-Dec-2010 11:10	116K	
avvdat-6194.zip	11-Dec-2010 11:10	75M	
avvdat.ini	11-Dec-2010 05:40	3.4K	

This zip file is regularly updated at *McAfee®* web site. Installing the file overwrites the current installed file and this file can be updated even if the antivirus application is scanning the system.

During every scan, the *RMX* system checks if there is a *DAT* file update. When the *DAT* file is not updated in the past 30 days, an active alarm is triggered: "*Antivirus initial DAT files are outdated and must be updated*". This alarm appears in the *Active Alarms* list. The active alarm terminates when the antivirus scan activates.

Downloading and Converting the ZIP file to TAR

Download the zip file to a local PC/laptop. The *McAffee* file is automatically converted to a *TAR* file with a .tgz file extension..

> Schedule signature file updates in accordance with your site policies.

Active Alarms

Table 3 lists the Active Alarms that can occur on the system.

Table 3   *Antivirus Active Alarms*

Active Alarm	Description
Virus scan in progress	RMX system is running a virus scan.
Invalid DAT (virus database) file	The DAT file downloaded onto the system is corrupt or invalid. Upload the file again.
A virus threat has been detected	A virus has been detected on the RMX.
Virus scan has been terminated by time-out	The Virus scan was terminated by a time-out on the RMX system.
Antivirus initial DAT files are outdated and must be updated	The Antivirus initial DAT files are outdated and must be updated on the RMX system.

Logger File Additions

New antivirus statuses have been added to registry of the *Logger Utility*. The following new antivirus statuses are written to the logger file:

- Scan start
- Scan end
- Scan schedule
- Scan schedule change
- Virus found
- *DAT* file update
- Any *Antivirus* alert

Direct Connection to Polycom RMX™ Serial Gateway S4GW

UC APL Public Key Infrastructure (*PKI*) requires that the *Serial Gateway S4GW* be connected directly to the *RMX* and not to the *H.323* network. The *Serial Gateway* effectively becomes an additional module of the *RMX*, with all web and *H.323* traffic passing through the *RMX*.

Figure 4 *Network infrastructure with direct connection to Serial Gateway S4GW*

After initial setup, the *Serial Gateway* is configured, managed and monitored via the *RMX Web Client / RMX Manger*. For more information see "*Setting Up Your Polycom RMX Serial Gateway S4GW*" in the *RMX Serial Gateway S4GW System User Guide.*

Guidelines

- The *Serial Gateway* is supported on *RMX 1500/2000/4000*.
- Only one *Serial Gateway* can be connected directly to an *RMX*.
- The *Serial Gateway* can be associated with only one *Network Service*.
- Although the *Media* and *Signaling Network Service* on the *RMX* can be configured for *IPv6* addressing, the *Network Service* assigned to the *Serial Gateway* can only support *IPv4* addressing.
- The following *System Flags* must be set to **YES**:
  — **ULTRA_SECURE_MODE**
  — **V35_ULTRA_SECURED_SUPPORT**
- When connecting the *Serial Gateway* to an *RMX 2000*:
  — It is essential that an *RTM LAN* card is installed.
  — The *Serial Gateway* must be physical connected to the RTM LAN card, *LAN 1* port.
  — The **SEPARATE_MANAGEMENT_NETWORK** *System Flag* must be set to **YES**.

- The following *System Flags* must be set to **NO**:
  - — **MULTIPLE_SERVICES**
  - — **ENABLE_EPC** (If this *System Flag* doesn't exist it must be created.)
- If *Content* is to be shared the conference *Profile* should have *Content Protocol* set to **H.263**.
- When the *RMX* is in *Ultra Secure Mode,* it requires that the *Serial Gateway* be in *Maximum Security Mode.* For more information see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments, "Serial Gateway S4GW - Maximum Security Mode"* on page **5-11**.
- *H.323* connections to the *RMX* are 1024-bit encrypted *TLS*.
- *RTP* traffic between the *RMX* and the *Serial Gateway* are not encrypted.
- The *Certificate* installed on the *Serial Gateway* must be also be installed in the workstation that is used to run the *RMX Web Client / RMX Manager*.
- Table 1-1 summarizes the *LAN* port connections for each of the *RMX* platforms.

Table 1-1   *LAN Port Connections per RMX Platform*

RMX	Management	Signaling	Media	V.35 Serial Gateway Direct Connection
1500	MNG B	MNG	LAN 2	**LAN 1**
2000	RTM IP LAN 3	RTM IP LAN 2	RTM IP LAN 2	**RTM LAN LAN 1**
4000	RTM IP LAN 2	RTM IP LAN 3	RTM LAN LAN 2	**RTM LAN LAN 1**

- When using a HDX endpoint, it should be configured as follows:

Configuring the RMX - Serial Gateway Connection

Configuring the connection between the *Serial Gateway* and the *RMX* consists of the following procedures:

1 **Initial Setup of the Serial Gateway**

    For more information see *"Setting Up Your Polycom RMX Serial Gateway S4GW"* in the *RMX Serial Gateway S4GW System User Guide*.

2 **Configure a Network Service on the RMX for the Serial Gateway and Connect the Serial Gateway to the RMX**.

These procedures are described in detail in *Chapter 5* of the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments*

> For a detailed description of these procedures see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments* "*Configuring the RMX - Serial Gateway Connection"* on page **5-2**.

Detailed Description - Changes to Existing Security Features

RMX Hardware

Version 7.5.0.J requires MPM+ or MPMx cards to be installed in the RMX.

Ultra Secure Mode Flag

Ultra Secure Mode, is enabled by manually adding the **ULTRA_SECURE_MODE** flag to the *System Configuration* and setting its value to **YES**.

Guidelines

- When upgrading from a version containing a **JITC_MODE** *System Flag*, the system will automatically create an **ULTRA_SECURE_MODE** *System Flag* and set it to the value of the **JITC_MODE** flag before the upgrade.

  The system will then delete the **JITC_MODE** *System Flag*.

- When downgrading to a version that utilizes the **JITC_MODE** *System Flag*, the administrator will need to set the **JITC_MODE** flag to the value of the **ULTRA_SECURE_MODE** flag's value before the upgrade

- Once intiated, *Ultra Secure Mode* cannot be disabled without restoring the *RMX* to factory defaults.

  For more information see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments*, *"Comprehensive Restore to Factory Defaults"* on page **4-1**.

Login Page/Main Page Banners

The administrator can choose one of four alternative login banners to be displayed. The four alternative banners cannot be modified. A *Custom* banner (default) can also be defined.

The *Main Page Banner* is blank and can be defined.

The *Banner Configuration* dialog box allows the administrator to select a *Login Banner* from a drop-down menu.
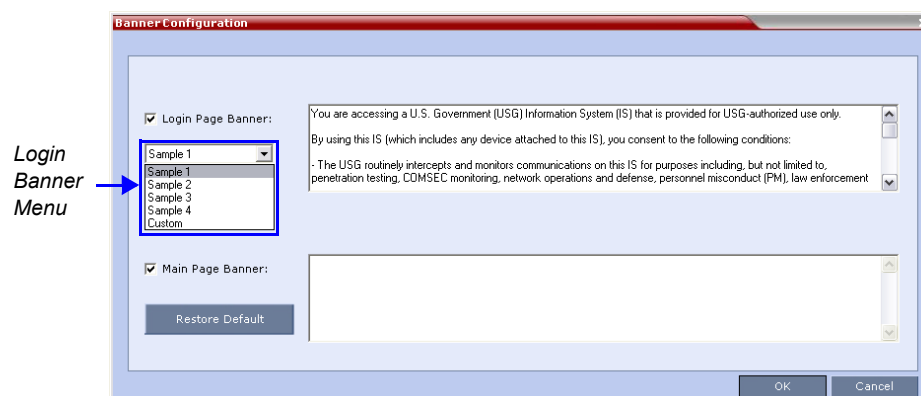
One of the the following *Login Banners* can be selected:

- **Non-Modifiable Banners**
  - *Sample 1*
  - *Sample 2*
  - *Sample 3*
  - *Sample 4*
- **Modifiable Banner**
  - *Custom* (Default)

Guidelines

- The *Login Banner* cannot be disabled when the *RMX* is in *Ultra Secure Mode*.
- The *Login Banner* must be acknowledged before the user is permitted to log in to the system.
- If a *Custom* banner has been created, and the user selects one of the alternative, non-modifiable banners the *Custom* banner not deleted.
- The *Custom Login Banner* banner may contain up to 1300 characters.
- An empty *Login Banner* is not allowed.
- Any attempt to modify a non-modifiable banner results in it automatically being copied to the *Custom* banner.

Non-Modifiable Banner Text

Sample 1 Banner

```
You are accessing a U.S. Government (USG) Information System (IS) that
is provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Sample 2 Banner

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users also may be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Sample 3 Banner

You are about to access a system that is intended for authorized users only. You should have no expectation of privacy in your use of this system. Use of this system constitutes consent to monitoring, retrieval, and disclosure of any information stored within the system for any purpose including criminal prosecution.

Sample 4 Banner

This computer system including all related equipment, network devices (specifically including Internet access), is provided only for authorized use. All computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized personnel and their entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information including personal information, placed on or sent over this system may be monitored. Use of this system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of any such unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

User Management

User Name - Case Sensitivity

User names are case sensitive.

Strong Passwords

User Passwords

Maximum Repeating Characters

A *System Flag* **MAX_PASSWORD_REPEATED_CHAR** allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a password.

Range: 1 - 4

Default: 2

Conference and Chairperson Passwords

Maximum Repeating Characters

A *System Flag* **MAX_CONF_PASSWORD_REPEATED_CHAR** allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a password.

Range: 1 - 4

Default: 2

> *Chairperson* users are not supported in *Ultra Secure Mode*.

USB Restore to Default

The *USB* port of an *RMX* in *Ultra Secure Mode* can be used to:

- Restore the *RMX* to *Factory Security Defaults* mode *(https → http).*
- Perform a *Comprehensive Restore to Factory Defaults*

Restore to Factory Security Defaults

Restore to Factory Security Defaults can be performed by either:

- Inserting a *USB* device such as a mouse or a keyboard into the *RMX's USB Port* causing it to exit *Ultra Secure Mode* and return to *Factory Security Defaults* mode. After performing this procedure, *Logins* to the *RMX* use the **http** command and not the **https** command.

  or

- Inserting a *USB* key containing a file named *RestoreFactorySecurityDefaults*.

To restore the RMX to Factory Security Defaults:

1 Insert a USB device or a *USB* key containing a file named *RestoreFactorySecurityDefaults* into the *USB* port of the *RMX*.

2 Power the *RMX* **Off** and then **On**.

3 Login using **http**://<Control Unit IP Address>.

Comprehensive Restore to Factory Defaults

Inserting a *USB* key containing a file named *RestoreToFactoryDefault* **and** a *lan.cfg* file will cause the *RMX* to exit *Secure Mode* **and** perform a *Comprehensive Restore to Factory Defaults*.

For more information see the *RMX 1500/2000/4000 Deployment Guide for Maximum Security Environments "Comprehensive Restore to Factory Defaults Procedure"* on page **4-4**.

V.35 Gateway Tab in IP Network Service Dialog Box

The IP Network Service dialog box for each IP Network Service, has a new tab,

V.35 Gateway, enabling the administrator to add the gateway to a new or existing IP Network Service.
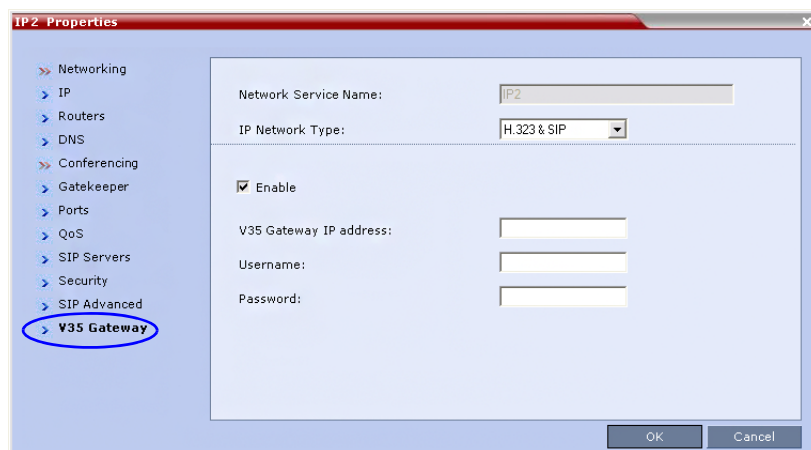
Additional Log Events

Firewall denials and errors pertaining to the *MCMS* will be logged by the *Logger* utility and *Auditor*.

Auditor users are not supported in *Ultra Secure Mode*.

Detailed Description - New Features

Gathering Phase

The *Gathering Phase* of a conference is the time period during which participants are connecting to a conference. During the *Gathering Phase*, a mix of live video from connected endpoints is combined with both static and variable textual information about the conference into a slide which is displayed on all connected endpoints. All connected participants are kept informed about the current conference status including names of connected participants, participant count, participant type (video/audio) etc.

During the *Gathering Phase*, the audio of all participants can be heard, and the video of active speakers is displayed in the video windows as they begin talking.

Textual Information — *Live Video From Connected Participants*

Recording Indicator Not Supported in Ultra Secure Mode

Connected Participants

Conference Information

Optional Additional Information (Info1/2/3 in Profile see page 1-97)

Access Numbers
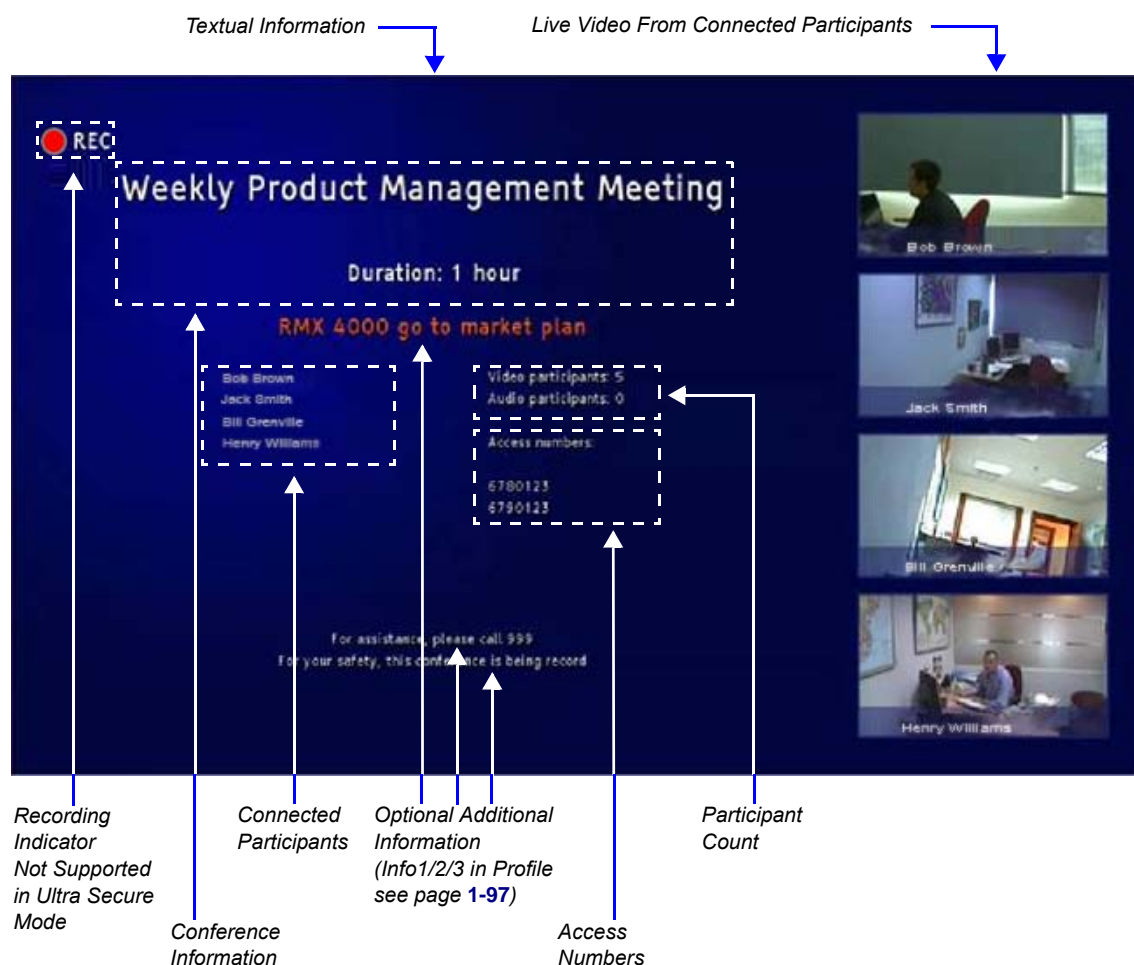
Participant Count

Gathering Phase Guidelines

- The *Gathering Phase* slide can be displayed at any time during the conference by entering the *Show Participants DTMF* code, ***88**.
- The *Gathering Phase* is not supported in *Video Switching Conferences*.
- The names of the first eight participants to connect are displayed. If eight or more participants connect, the 8th row displays "**...**".

- **Static text** in the *Gathering Phase* slide such as the field headings: *Organizer, Duration, Video/Audio Participants, Access Number, IP* are always displayed in the language as configured in the *Polycom Virtual Meeting Rooms Add-in for Microsoft Outlook*.

- The following languages are supported:
  — English
  — French
  — German
  — International Spanish
  — Korean
  — Japanese
  — Simplified Chinese

- **Dynamic text** in the *Gathering Phase* slide such as the meeting name, participants names, access numbers and the additional information entered in the *Info1/2/3* fields of the *Gathering Settings* tab of the conference *Profile* are displayed in the language of the meeting invitation.

- The language of a *Gathering Phase* slide of a conference configured to include a *Gathering Phase* that is not launched by the *Polycom Conferencing Add-in for Microsoft Outlook* is configured by the administrator. Using the *RMX Web Client,* the administrator selects the language for the *Gathering Phase slide.* The language selected can be different to that of the *RMX Web Client* used by the administrator to perform the configuration.

- *Content* can be sent during the *Gathering Phase.* The content is displayed in the large video window of the participant's layout while the *Gathering* slide is displayed in a smaller video window in the layout.
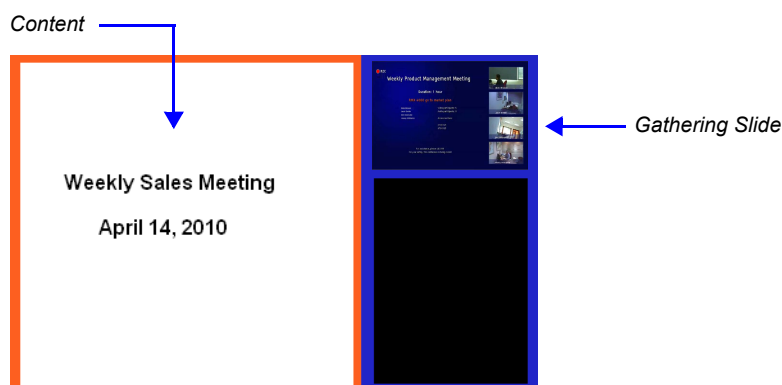
Gathering Phase Duration

The duration of the *Gathering Phase* can be customized by the administrator so that it is long enough to be viewed by most connected participants yet short enough so as not to over extend into the scheduled conferencing time.

The *Gathering Phase* duration is configured for the *RMX*, by the following *System Flags* in *system.cfg* using the *Setup >System Configuration* menu:

- **CONF_GATHERING_DURATION_SECONDS**

  Range: 0 - 3600 seconds

  Default: 180 seconds

  The *Gathering Phase* duration of the conference is measured from the scheduled start time of the conference.

Example: If the value of the flag is set to **180**, the *Gathering* slide is displayed for three minutes to all participants starting at the conference *Start Time*, and ending three minutes after the conference *Start Time*.

For participants who connect before *Start Time*, the *Gathering* slide is displayed from the time of connection until the end of the *Gathering* duration period.

- **PARTY_GATHERING_DURATION_SECONDS**

  Range: 0 - 3600 seconds

  Default: 15 seconds

  The value of this flag determines the duration of the display of the *Gathering* slide for participants that connect to the conference after the conference *Start Time*.

  Participants connecting to the conference very close to of the end of the *Gathering Phase* (when there are fewer seconds left to the end of the *Gathering Phase* than specified by the value of the flag) have the *Gathering* slide displayed for the time specified by the value of the flag.

  Example: If the value of the flag is set to **15**, the *Gathering Phase* slide is displayed to the participant for 15 seconds.

Enabling the Gathering Phase Display

The *Gathering Phase* is enabled for per conference in the *Conference Profile*. The profile also includes the dial-in numbers and the optional additional information to display on the slide.

Conferences that are configured to include a *Gathering Phase* that are not launched by the *Polycom Conferencing Add-in for Microsoft Outlook* need the following information to be entered via the *New Profile* or *Profile Properties – Gathering Settings* dialog box:
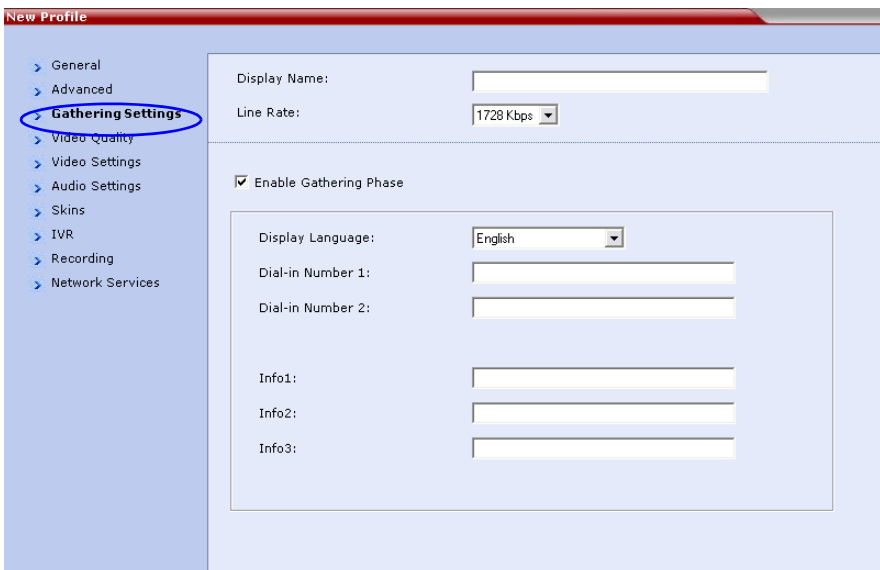
- *Display Name*   (Optional, the *Meeting Name* is used if left blank.)
- *Displayed Language*
- *Access Number 1 / 2*   (Optional.)
- Additional Information   (Optional free text)
  - *Info 1*
  - *Info 2*
  - *Info 3*

Conferences launched by the *Polycom Conferencing Add-in for Microsoft Outlook* receive this information from the meeting invitation.

To enable the Gathering Phase:

1   In the *RMX Management* pane, click **Conference Profiles**.

2   In the *Conference Profiles* pane, click the **New Profile** button or double-click the entry of an existing profile to be modified.

3   Click the **Gathering Settings** tab.

4   Define the following fields:

Table 2   *Profile - Gathering Settings*

Field	Description
Display Name	This field is defined when the *Profile* is created. For more information see the *RMX 2000/4000 Administrator's Guide*, "*Defining Profiles"* on page **1-9**.
Enable Gathering	Select this check box to enable the *Gathering Phase* feature. Default: Selected.
Displayed Language	Select the *Gathering Phase* slide language: *Gathering Phase* slide field headings are displayed in the language selected. The *Gathering Phase* slide can be in a different language to the *RMX Web Client*. Default: English **Note:** When working with the *Polycom Conferencing Add-in for Microsoft Outlook,* the language selected should match the language selected for the conference in the *Polycom Conferencing Add-in for Microsoft Outlook* to ensure that the *Gathering Phase* slide displays correctly.
Access Number 1 *Access Number 2*	Enter the ISDN or PSTN number(s) to call to connect to the conference. Note: The numbers entered must be verified as the actual Access Numbers.

Table 2   *Profile - Gathering Settings*

Field	Description
Info 1	Optionally, enter any additional information to be displayed during the Gathering Phase.
	These fields are not limited in the RMX Web Client but only 96 characters can be displayed in the Gathering Slide on a 16:9 monitor.
Info 2	If the Gathering slide is displayed on a 4:3 endpoint: the slide is cropped on both sides:
	• The left most characters of the information fields will not be displayed.
	• The live video is cropped on the right side of the display.
Info 3	
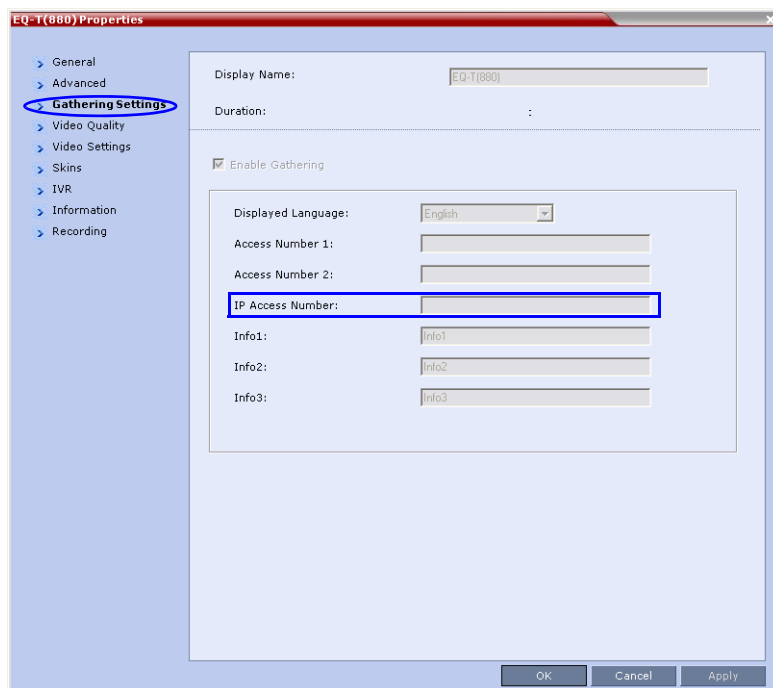
5   Click OK.

Monitoring Gathering-enabled Conferences

Conferences launched by the *Polycom Conferencing Add-in for Microsoft Outlook* are monitored in the same manner as all other conferences.

In the gathering settings tab, an additional field, *IP Access Number,* is displayed in addition to the ISDN/PSTN access numbers, *Access Number 1* and *Access Number 2* which were entered when defining the conference *Profile*.

The *IP Access Number* is made up of the *Conference ID* generated by the *Polycom Conferencing Add-in for Microsoft Outlook* and the gatekeeper prefix.

Auto Brightness

Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.

Guidelines

- *Auto Brightness* is supported with *MPM+* and *MPMx* cards only.
- *Auto Brightness* only increases brightness and does not darken video windows.
- *Auto Brightness* is enabled by the **SET_AUTO_BRIGHTNESS** *System Flag* in *system.cfg* using the **Setup >System Configuration** menu.
  Possible Values: ON / OFF
  Default: OFF

Audio Clarity

Audio Clarity improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity.

The enhancement is applied to the following low bandwidth (4kHz) audio algorithms:

- G.729a
- G.711

Guidelines

- *Audio Clarity* is supported with *MPM+* and *MPMx* cards only.
- *Audio Clarity* is enabled by the **SET_AUDIO_CLARITY** *System Flag* in *system.cfg* using the **Setup >System Configuration** menu.

    Possible Values: ON / OFF

    Default: OFF

Packet Loss Concealment (PLC) for Audio

Packet Loss Concealment (*PLC*) for *Siren* audio algorithms improves received audio when packet loss occurs in the network.

The following audio algorithms are supported:

- Siren 7 (mono)
- Siren 14 (mono/stereo)
- Siren 22 (mono/stereo)

Guidelines

- *PLC for Audio* is supported with *MPM+* and *MPMx* cards only.
- The speaker's endpoint must use a *Siren* algorithm for audio compression.
- *PLC* is enabled by the **SET_AUDIO_PLC** *System Flag* in *system.cfg* using the **Setup >System Configuration** menu.
  Possible Values: ON / OFF
  Default: ON

Siren 22 and G.719 Audio Algorithm Support

Polycom's proprietary *Siren 22* and industry standard *G.719* audio algorithms are supported for participants connecting with *Polycom* endpoints.

The *Siren 22* Audio Algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications. Siren 22 requires dramatically less computing power and has much lower latency than alternative wideband audio technologies.

Guidelines

- *Siren 22, G.719* and *Siren 22Stereo* are supported with *MPMx* cards only.
- *Siren 22* and *G.719* are supported in both mono and stereo.
- Stereo is supported in *H.323* calls only.
- *Siren 22* is supported by Polycom HDX endpoints, Version 2.0 and later.

Mono

The *Siren 22* and *G.719* mono audio algorithms are supported at the following bit rates:

Table 3   *Siren22 and G.719 Mono vs Bitrate*

Audio Algorithm	Minimum Bitrate (kb)
Siren22 64k	384
Siren22 48K	
Siren22_32k	
G.719_64k	
G.719_48k	
G.719_32k	
Siren22_48K	256
Siren22_32k	
G.719_48k	
G.719_32k	
Siren22_32k	128
G.719_32k	

Stereo

The *Siren 22Stereo* and *G.719Stereo* audio algorithms are supported at the following bit rates.

Table 4   *Siren22Stereo and G.719Stereo vs Bitrate*

Audio Algorithm	Minimum Bitrate (kb)
Siren22Stereo_128k	1024
*Siren22*Stereo_96k	
*Siren22*Stereo_64k	
G.719Stereo_128k	
G.719Stereo_96k	
G.719Stereo_64k	
*Siren22*Stereo_96k	512
*Siren22*Stereo_64k	
G.719Stereo_96k	
G.719Stereo_64k	
Siren22Stereo_64k	384
G.719Stereo_64k	

Monitoring Participant Audio Properties

The audio algorithm used by the participant's endpoint can be verified in the Participant Properties - Channel Status dialog box.

To view the participant's properties during a conference:

1   In the *Participants* list, right click the desired participant and select **Participant Properties**.

2   Click the **Channel Status - Advanced** tab.
     The *Participant Properties - Channel Status - Advanced* dialog box is displayed.

3   In the *Channel Info* field, select **Audio In** or **Audio Out** to display the audio parameters.

4   Click the **OK** button.

H.264 High Profile

The *H.264 High Profile* is a new addition to the *H.264* video protocol suite. It uses the most efficient video data compression algorithms to reduce bandwidth requirements for video data streams.

Video quality is maintained at bit rates that are 20% to 30% lower than previously required. For example, a 832kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.

Guidelines

- *H.264 High Profile* is supported with *MPMx* cards only.
- *H.264 High Profile* is supported in *H.323, SIP* and *ISDN* networking environments.
- *H.264 High Profile* is supported in *Continuous Presence* conferences at all bit rates, video resolutions and layouts.
- *H.264 High Profile* is the first protocol declared by the *RMX*, to ensure that endpoints that support the protocol will connect using it.
- For monitoring purposes, the *RMX* and endpoint *H.264 High Profile* capability is listed in the *Participant Properties - H.245* and *SDP* tabs for *H.323* participants and *SIP* participants respectively.

  For more information see the *RMX 1500/2000/4000 Administrator's Guide*, on page "IP Participant Properties" on page **11-19**.

The *H.264 High Profile* is a new addition to the *H.264* video protocol suite. It uses the most efficient video data compression algorithms to reduce bandwidth requirements for video data streams.

Video quality is maintained at bit rates that are 20% to 30% lower than previously required. For example, a 832kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.

Guidelines

- *H.264 High Profile* is supported with *MPMx* cards only.
- *H.264 High Profile* is supported in *H.323, SIP* and *ISDN* networking environments.
- *H.264 High Profile* is supported in *Continuous Presence* conferences at all bit rates, video resolutions and layouts.
- *H.264 High Profile* is the first protocol declared by the *RMX*, to ensure that endpoints that support the protocol will connect using it.

> H.264 High-Profile should be used when all or most endpoints support it.

Setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile.*

- For monitoring purposes, the *RMX* and endpoint *H.264 High Profile* capability is listed in the *Participant Properties - H.245* and *SDP* tabs for *H.323* participants and *SIP* participants respectively.

  For more information see the *RMX 1500/2000/4000 Administrator's Guide*, "IP Participant Properties" on page **11-19**.

- *H.264 High Profile* is not supported:
  — In *MPM+* card *Configuration Modes*
  — In *Video Switched* conferences

— For *Content Sharing*
— As an *RSS Recording* link
— With *Video Preview*

H.264 High Profile System Flags

ISDN

The **CFG_KEY_SUPPORT_HIGH_PROFILE_WITH_ISDN** *System Flag* enables *ISDN* support with *H.264 High Profile*.

Possible Values: YES / NO

Default: NO

This *System Flag* must be added to the *System Configuration* file before it can be modified. For more information see the *RMX 15002000/4000 Administrator's Guide*, "*Modifying System Flags*" on page **19-6**.

Flags used in Version 7.0.1

In *Version 7.0.2* the flags described below were replaced with the *High Profile* sliders in the *Resolution Configuration* dialog box.

Setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile*.

Endpoints that do not support *H.264 High Profile* will connect according to the minimum bitrate thresholds defined by the following *System Flags*:

• H264_BASE_PROFILE_MIN_RATE_SD30_SHARPNESS
• H264_BASE_PROFILE_MIN_RATE_HD720P30_SHARPNESS
• H264_BASE_PROFILE_MIN_RATE_HD1080P30_SHARPNESS
• H264_BASE_PROFILE_MIN_RATE_CIF60_MOTION
• H264_BASE_PROFILE_MIN_RATE_SD60_MOTION
• H264_BASE_PROFILE_MIN_RATE_HD720P60_MOTION

These *System Flags* must be added to the *System Configuration* file before they can be modified. For more information see the *RMX 15002000/4000 Administrator's Guide*, "*Modifying System Flags*" on page **19-6**.

Example: If the *High Profile Optimized* option is selected in the *Resolution Configuration* dialog box and the *System Flag* values are set as in the following table:

System Flag	Default Value
H264_BASE_PROFILE_ MIN_RATE_SD30_SHARPNESS	256
H264_BASE_PROFILE_ MIN_RATE_HD720P30_SHARPNESS	1024
H264_BASE_PROFILE_ MIN_RATE_HD1080P30_SHARPNESS	1536
H264_BASE_PROFILE_ MIN_RATE_CIF60_MOTION	256

System Flag	Default Value
H264_BASE_PROFILE_ MIN_RATE_SD60_MOTION	1024
H264_BASE_PROFILE_ MIN_RATE_HD720P60_MOTION	1536

Endpoints will connect at resolutions as set out in the following table, depending on whether they support *H.264 High Profile* or not:

Video Quality Setting	Endpoint Connection Bit Rate (kbps)		Resolution
	High Profile Supported	**High Profile Not Supported**	
Sharpness	**128**<= bit rate <**512**	**256**<= bit rate <**1024**	SD30
	512<= bit rate <**1024**	**1024**<= bit rate <**1536**	HD720P30
	1024<= bit rate	**1536**<= bit rate	HD1080P30
Motion	**128**<= bit rate <**512**	**256**<= bit rate <**1024**	CIF60
	512<= bit rate <**832**	**1024**<= bit rate <**1536**	SD60
	832<= bit rate	**1536**<= bit rate	HD720P60

For more information see the *RMX 15002000/4000 Administrator's Guide*, *"Modifying System Flags"* on page **19-6**.

New Symmetric HD Resolutions in MPMx Mode

MPMx mode, supports the following new HD video resolutions in both *Continuous Presence* and *High Definition Video Switching* modes.

- **HD 1080p30** (symmetric) – endpoints send HD 1080p at 30 fps and receive HD 1080 at 30 fps
- **HD 720p60** (symmetric) – endpoints send HD720 at 60 fps and receive HD720 at 60 fps

These resolutions are available at line rates of 128 to 8192 Kbps depending on Flag and Resolution Slider settings. For more information, see "System Flag" on page **1-111**.

- Depending on the line rate, the RMX sends video at the best possible resolution supported by the endpoint regardless of the resolution received from the endpoint.

> - The video resolution transmitted to any endpoint is determined by the endpoint's capabilities, the conference line rate, the Conference Profile's Motion and Sharpness settings and the RMX's Card Configuration Mode (MPM+ or MPMx).
> - The frames per second (fps) values listed for the video resolutions above are the maximum possible and may be adjusted downward depending on available bandwidth.

Table 5 and Table 6 show the relationship between minimum line rate threshold and video quality for both *Motion* and *Sharpness* settings in both *MPM+* and *MPMx Card Configuration Modes*.

Table 5 MPMx: Video Quality vs Minimum Line Rate Threshold

Resolution	Line Rate (kbps)							
	Balanced (Default)		Resource Optimized		Video Quality Optimized		High Profile Optimized	
	Sharp-ness	Motion	Sharp-ness	Motion	Sharp-ness	Motion	Sharp-ness	Motion
HD1080p30	4096		4096		1560		1024	
HD720p30	1024		1920		768		512	
SD30	256		384		256		128	128
HD720p60		1920		1920		1560		832
SD60		1024		1024		768		512
WCIF60		384		384		256		

Table 6 MPM+: Video Quality vs Minimum Line Rate Threshold

Resolution	Line Rate (kbps)					
	Balanced (Default)		Resource Optimized		Video Quality Optimized	
	Sharp-ness	Motion	Sharp-ness	Motion	Sharp-ness	Motion
HD1080p30	4096		4096		1560	
HD720p30	1024		1920		768	
SD30	256		384		256	
HD720p60		1920		1920		1560
SD60		1024		1024		768
WCIF60		384		384		256

Resource Usage

The RMX uses video ports to connect HD endpoints as follows:

- 4 video (CIF) ports are used to connect each endpoint capable of receiving *HD 720p30.*
- 8 video (CIF) ports are used to connect each endpoint capable of receiving *HD 1080p30* or *HD 720p60.*

System Flag

The **MAX_CP_RESOLUTION** flag value is applied to the system during *First Time Power-on* and after a system upgrade. The default value is *HD1080.*

All subsequent changes to the maximum *CP* resolution of the system are made by selections in the *Resolution Configuration* dialog box.

For more information see "*Resolution Configuration*" on page 130.

Additional Call Rates

The line rates summarized in Table 1 have been added to give administrators more control over bandwidth utilization.

Table 7   *Line Rate by Conferencing Mode / MPM Card Type*

Line Rate (kbps)	MPM+	MPMx
192		
320		
832		
1280	Continuous Presence / Video Switching	
1728		
2048		
2560		
3072		
3584		
6144	Not Supported	Video Switching

Guidelines

- *ISDN* endpoints are connected at the highest bonded line rate below the selected conference line rate. For example: If the conference line rate is 1024kbps, the participant is connected at 768kbps.
- Each *LAN* connection to the *RMX* has a maximum data rate capacity of 320Mbps. The maximum *LAN* capacities per *RMX* are summarized in Table 8:

Table 8   *RMX - Maximum Data Rates*

RMX Model	Number of LAN Connections	Maximum Data Rate Capacity Mbps
RMX 2000	*1*	320
RMX 2000 (with Multiple Networks)	2	640
RMX 4000	4	1280

H.239 / People+Content

The *H.239* protocol allows compliant endpoints to share content. All Conferences, Entry Queues, and Meeting Rooms launched on the *RMX* have *H.239* capability.

People+Content utilizes a different signaling protocol and is *Polycom's* proprietary equivalent of *H.239*.

Guidelines

- *H.323* environment is supported.
- Conferences can include a mix of endpoints that support *H.239* or *People+Content*.
- All endpoints will receive Content at the highest resolution common to all connected endpoints.
- *SIP People+Content* is supported with *MPM+* and *MPMx* cards.
- *H.239* is supported in *MIH*, *Star* and *Basic Cascading* topologies.
- *People+Content* is supported in cascaded conferences but cannot be used as the protocol for a cascade link.
- If an endpoint supports both *H.239* and *People+Content* protocols, *H.239* is selected as the preferred communications protocol.
- *People+Content* is enabled by default. It can be disabled for all conferences and endpoints by manually adding the **ENABLE_EPC** *System Flag* to the *System Configuration* and setting its value to **NO** (default setting is **YES**).
- Endpoints that support *People+Content* (for example, *FX* endpoints) may require a different signaling protocol. For these endpoints, manually add the *System Flag* **CS_ENABLE_EPC** to the *System Configuration* and set its value **YES** (default value is **NO**).

G.728 Audio Algorithm Support

Industry standard *G.728* audio algorithm is supported for participants connecting with legacy or low bandwidth endpoints.

Guidelines

G.728 is supported:
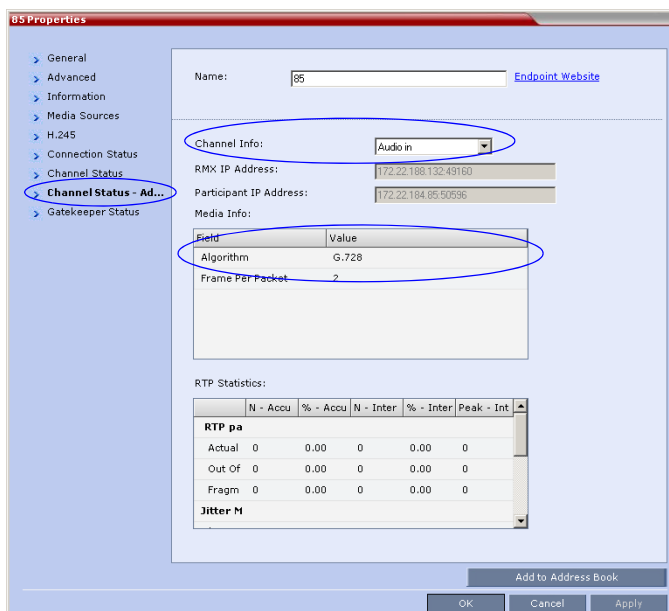
- with *MPM+* cards only
- in mono
- in *H.323* and *ISDN* networking environments
- at bitrates from 64kbps to 4096kbps

Monitoring Participant Audio Properties

The audio algorithm used by the participant's endpoint can be verified in the Participant Properties - Channel Status dialog box.

To view the participant's properties during a conference:

1   In the *Participants* list, right click the desired participant and select **Participant Properties**.

2   Click the **Channel Status - Advanced** tab.
      The *Participant Properties - Channel Status - Advanced* dialog box is displayed.

3   In the *Channel Info* field, select **Audio In** or **Audio Out** to display the audio parameters.

4   Click the **OK** button.

Permanent Conference

A *Permanent Conference* is an ongoing conference with no pre-determined *End Time* continuing until it is terminated by an administrator, operator or chairperson.

> *Chairperson* users are not supported in *Ultra Secure Mode*.

Guidelines

• Resources are reserved for a *Permanent Conference*, only when the conference has become ongoing.

• Resources are allocated to a *Permanent Conference* according to the *Reserve Resources for Video Participants* field. If the number of defined dial-out participants exceeds the value of this field, the *RMX* automatically replaces the number in the *Reserve Resources for Video Participants* field with the number of defined dial-out participants in the *Permanent Conference.*

• *Auto Terminate* is disabled in *Permanent Conferences*.

• If participants disconnect from the *Permanent Conference,* resources that were reserved for its video and audio participants are released.

- *Ad-hoc Entry Queues*, *Conference Reservations* and *SIP Factories* cannot be defined as *Permanent Conferences*.
- Additional participants can connect to the conference, or be added by the operator, if sufficient resources are available.
- The maximum size of the *Call Detail Record* (*CDR*) for a *Permanent Conference* is 1MB.

Enabling a Permanent Conference

The *Permanent Conference* option is selected in the *New Conference, New Meeting Room* or *New Conference Templates* dialog boxes.

New Conference   New Meeting Room   New Conference Template
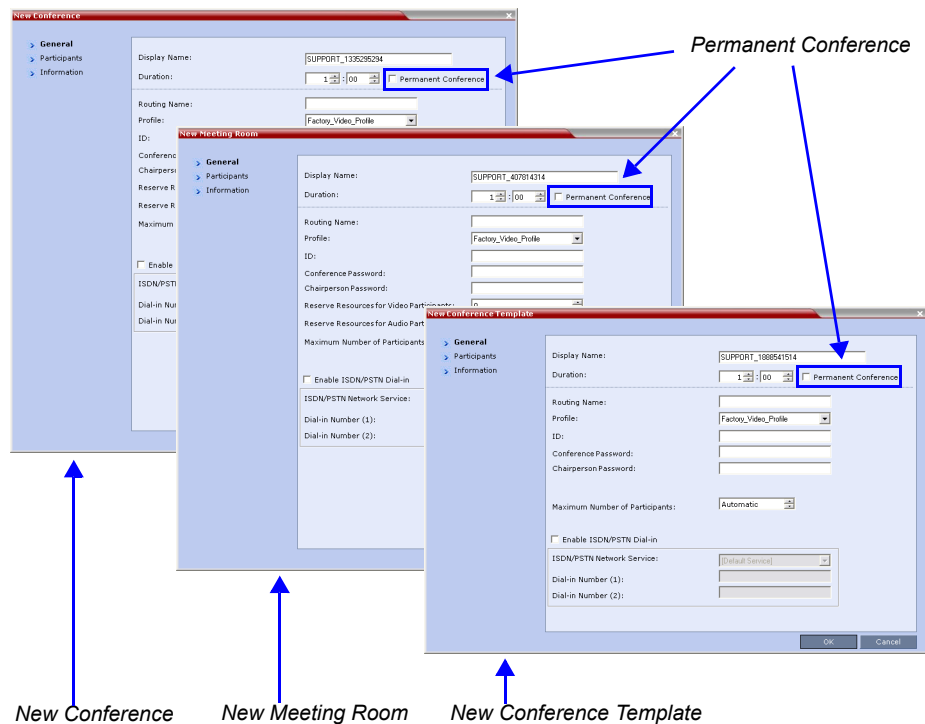
Video Preview

RMX users can preview the video sent from the participant to the conference (MCU) and the video sent from the conference to the participant. It enables the RMX users to monitor the quality of the video sent and received by the participant and identify possible quality degradation.

The video preview is displayed in a separate window independent to the RMX Web Client. All Web Client functionality is enabled and conference and participant monitoring as well as all other user actions can be performed while the video preview window is open and active.

Live video is shown in the preview window as long as the window is open. The preview window closes automatically when the conference ends or when participant disconnects from the conference. It can also be closed manually by the RMX user.

Video Preview Guidelines

- Video preview is available in *Continuous Presence* and *Video Switching* conferences.
- Video preview window size and resolution are adjusted to the resolution of the PC that displays the preview.
- Video Preview of the video sent from the conference to the participant is shown according to the line rate and video parameters of the level threshold to which the participant is connected.
- In versions up to and including Version 7.2.2, only users with Administrator authorization could request to view a video preview.
- Video preview is supported with MPM+ and MPMx cards.
- Only one preview window can be displayed for each RMX Web Client connection (workstation).
- Only one preview window can be displayed for a single conference and up to four preview windows can be displayed for each media card on different workstations (one per workstation and one per conference).
  For example, if the RMX contains two media cards, and there are 5 conferences running on the RMX, if five conferences are running on the same media card, only four conferences can be previewed from four different workstations. If four or less conferences are running on one media card and the remaining conferences are running on the other media card, all five conferences can be previewed.
- Live video that is shown in the preview window does not include the Content when it is sent by the participant.
- Video Preview is supported in cascaded conferences.
- If the video preview window is opened when the IVR slide is displayed to the participant, it will also be displayed in the video preview window.
- Video Preview is not supported in RMX Manager application.
- Video Preview is not supported with *H.264 High Profile*
- Video Preview is not supported for *RTV* endpoints.
- Video Preview is disabled in encrypted conferences.
- Video preview cannot be displayed when the participant's video is suspended.
- Participant's video preview and the CMAD window cannot be open and running simultaneously on the same PC as both require the same DirectDraw resource.

Workstation Requirements

To be able to display the video preview window, the following minimum requirements must be met:

- Windows XP and later
- Internet Explorer 7
- DirectX is installed
- DirectDraw Acceleration must be enabled and no other application is using the video resource
- Hardware acceleration must be enabled

Testing your Workstation

To ensure that your workstation can display the video preview window:

1 In Windows, click **Start > Run**.
   The *Run* dialog box opens.

2 In the *Open* field, type **dxdiag** and press the **Enter** key or click **OK**.
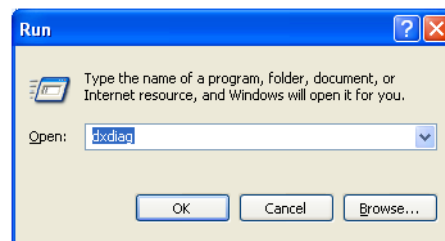
A confirmation message is displayed.

3 Click **Yes** to run the diagnostics.
   The *DirectX Diagnostic Tool* dialog box opens.

4 Click the **Display** tab.

To be able to display the video preview window, the **DirectDraw Acceleration** and **Direct3D Acceleration** options must be **Enabled**.
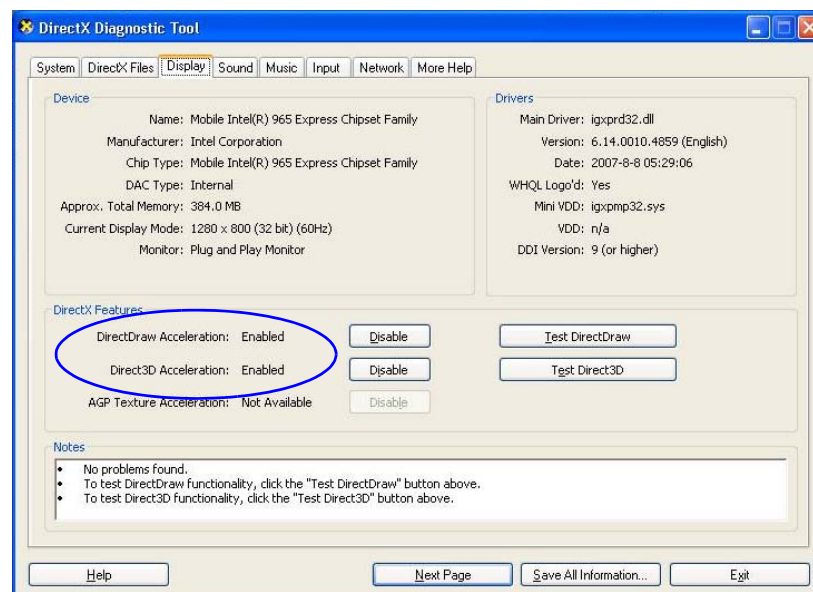
If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed in the Video Preview window.

5   Click the **Exit** button.

Previewing the Participant Video

To preview the participant video:

1   List the conference participants in the *Participants* pane.

2   Right-click the participant whose video you want to preview and then click one of the following options:
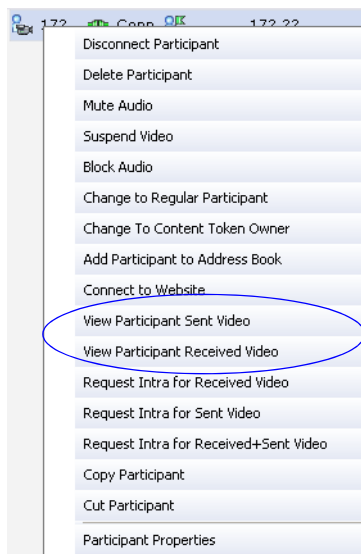
— **View Participant Sent Video** - to display the video sent from the participant to the conference.

— **View Participant Received Video** - to display the video sent from the conference to the participant.

The *Video Preview* window opens.
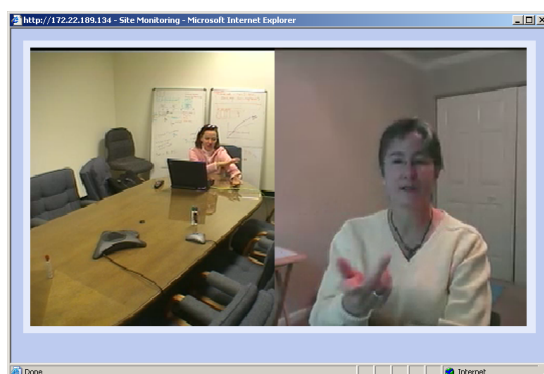
If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed.

For more a full description of *Click&View*, see the *RMX 1500/2000/4000 Getting Started Guide*, *"Personal Layout Selection with Click&View"* on page **3-83**.

Message Overlay

Message Overlay allows messages to be sent to all participants in an ongoing conference.

A maximum of 24 Unicode characters can be sent as a *Message Overlay*.
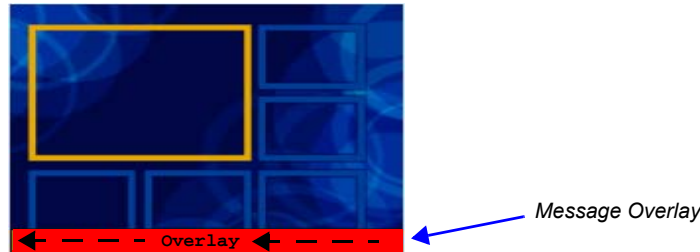
Message Overlay

Guidelines

- *Message Overlay* is supported in:
  — continuous Presence (CP) conferences
  — in *Same Layout* mode
  — in encrypted conferences
- *Message Overlay* is not supported in *Lecture* mode.
- Participants that have their video suspended do not receive *Message Overlays*.
- *Message Overlays* cannot be sent via the *Content* channel.
- *Message Overlay* is not displayed when the *PCM* menu is active.
- If a *Repeating Message Overlay* is modified before it has completed all its repetitions, it is changed immediately without completing all of its repetitions. The modified *Repeating Message Overlay* is displayed starting with repetition one.
- *Message Overlay* can be enabled, modified and disabled during an ongoing conference using the *Conference Properties – Message Overlay* dialog box.
- In some languages, for example Russian, when large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.

Enabling Message Overlay

Message Overlays are created and enabled in the *Conference Properties – Message Overlay* dialog box.

To enable Message Overlay:

1 In the *Conferences List* pane, double click the name of the conference to have *Message Overlay* enabled or right-click the conference name and then click **Conference Properties**.

    The *General* tab is displayed.

2 Click the **Message Overlay** tab.

The **Message Overlay** tab is displayed.
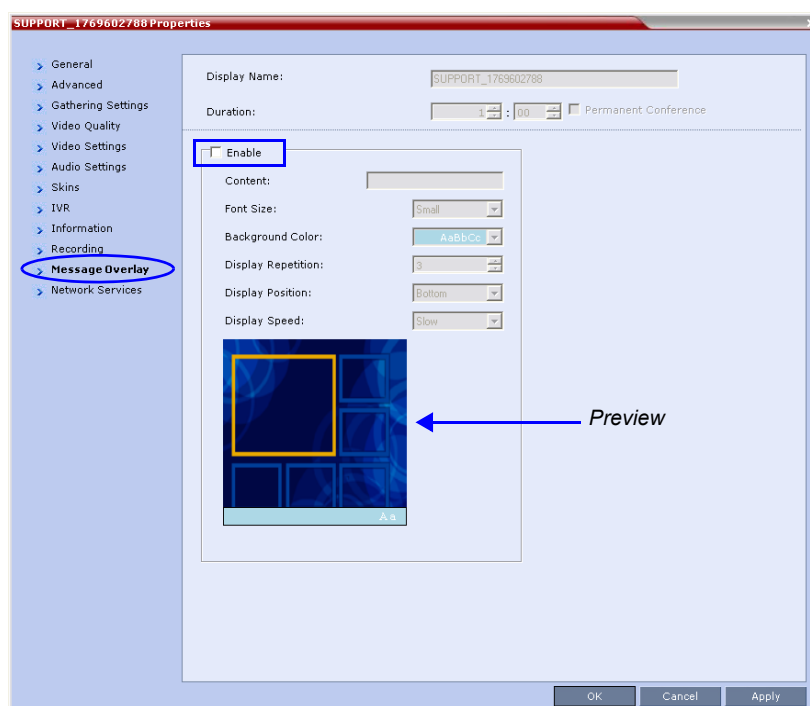
3 Select the **Enable** check box.

4 Modify the following fields as set out in Table 11.

As the fields are modified the *Preview* changes to show the effect of the changes.
For example:

Small Text, White on red, Top, Middle   *Small Text, White on yellow, Bottom*
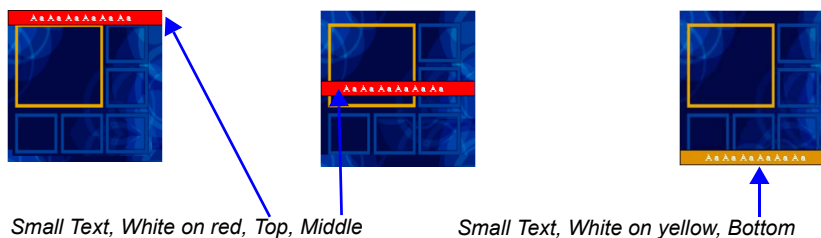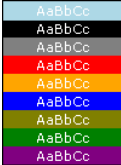
Table 9   *Conference Properties - Message Overlay*

Field	Description
Content	Enter a message of up to 24 Unicode characters.
Font Size	Select the size of the Message Overlay text from the drop-down menu options: • Small • Medium • Large **Default:** Small **Note:** In some languages, for example Russian, when large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.

Table 9   *Conference Properties - Message Overlay (Continued)*

Field	Description
Color	Select the color of the text and background of the Message Overlay from the following drop-down menu options: AaBbCc AaBbCc AaBbCc AaBbCc AaBbCc AaBbCc AaBbCc AaBbCc AaBbCc **Default:** White text on pale blue background
Display Repetition	Click the arrows (⬍) to increase or decrease the number of times that the Message Overlay is to be repeated. **Default:** 3
Display Position	Select the position for the display of the Message Overlay on the endpoint screen: • Top • Middle • Bottom **Default:** Bottom
Display Speed	Select whether the Message Overlay is static or repeating: • Static • Slow • Fast **Default:** Slow

5   Click the **OK** button.

Content Broadcast Control prevents the accidental interruption or termination of H.239 Content that is being shared in a conference.

Content Broadcast Control

Content Broadcast Control prevents the accidental interruption or termination of *H.239 Content* that is being shared in a conference.

Content Broadcast Control achieves this by giving *Content Token* ownership to a specific endpoint via the *RMX Web Client*. Other endpoints are not able to send content until *Content Token* ownership has been transferred to another endpoint via the *RMX Web Client*.

Guidelines

- *Content Broadcast Control* is supported in *MPM+* and *MPMx* card configuration modes.
- *Content Broadcast Control* is supported in *CP* and *Video Switching* conferences.
- *Content Broadcast Control* is supported in H.323 environments.
- Only the selected *Content Token* owner may send content and *Content Token* requests from other endpoints are rejected.
- *Content Token* ownership is valid until:
  — It is canceled by an administrator, operator or chairperson using the *RMX Web Client.*
  — The owner releases it.
  — The endpoint of the *Content Token* owner disconnects from the conference.
- An administrator, operator or chairperson can cancel *Content Token* ownership.

In cascaded conferences, a participant functioning as the cascade link cannot be given token ownership.

Chairperson users are not supported in *Ultra Secure Mode*.

Giving and Cancelling Token Ownership

Giving Token Ownership

To give token ownership:
1 In the *Participants* list, right click the endpoint that is to receive *Content Token* ownership.
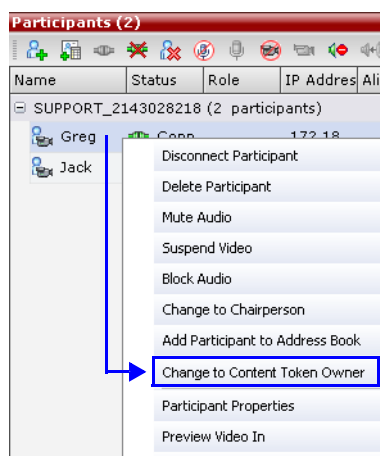
2   Select **Change To Content Token Owner** in the drop-down menu.

The endpoint receives ownership of the *Content Token* and an indication icon is displayed in the Role column of the participant's entry in the Participants list.
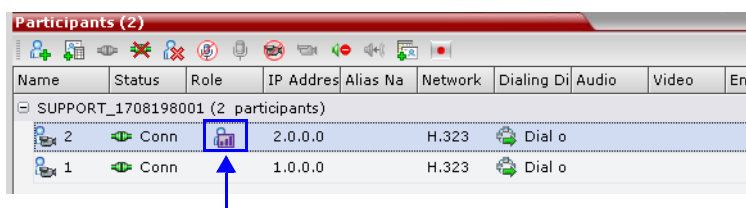
Cancelling Token Ownership

To cancel token ownership:

1   In the *Participants* list, right click the endpoint that currently has *Content Token* ownership.
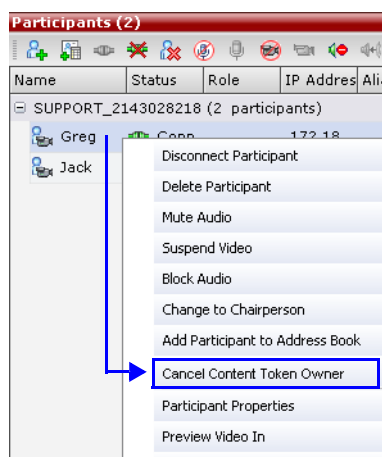
2   Select **Cancel Content Token Owner** in the drop-down menu**.**

Content Token ownership is cancelled for the endpoint.

Copy Cut and Paste Participant

The *RMX* user can **Copy**, **Cut** and **Paste** participants between differ rent conferences running on the *RMX,* including his/her current conference. These functions, when used via the *RMX Manager*, with its ability to manage multiple *RMX*s, participants, allows the *RMX* user to **Copy**, **Cut** and **Paste** participants between conferences running on different *RMX*s.

Copy Participant

The **Copy** command copies all the participant's properties and makes them available for pasting. The participant remains connected to his/her current conference.

To copy a participant:

1   In the *Participants List* pane, right-click the participant you want to copy.

2   In the drop-down menu select **Copy Participant**.
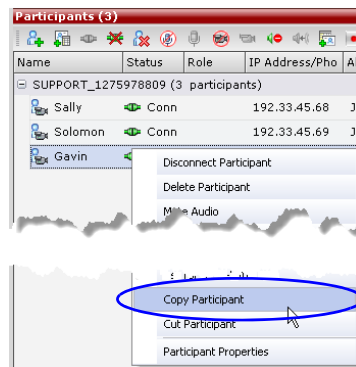
Cut Participant

The **Cut** command copies all the participant's properties and makes them available for *pasting*. The participant is deleted from his/her current conference.

To cut a participant:

1   In the *Participants List* pane, right-click the participant you want to cut.

2   In the drop-down menu select **Cut Participant**.
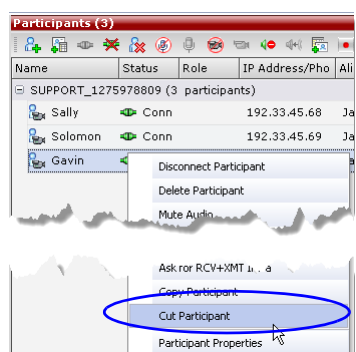
Paste Participant

The **Paste** command connects the *copied* or *cut* participant to the selected conference. If the participant was *copied*, he/she should be deleted from the conference he/she was *copied* from, unless it is required that the participant is connected to two (or more) conferences. (There are endpoints that permit a participant to be connected to multiple conferences).

To paste a participant:

1   In the *Conferences List* pane, click the conference you want to paste the copied/cut participant into.

2   Right-click in the *Participants List* pane of the selected conference and in the drop-down menu select **Paste Participant**.

    or

    If you are using the *RMX Manager* and you want to paste the participant to a conference to different *RMX*:

    a   In the *MCUs* list pane, click the *RMX* that is hosting the conference that is to receive the participant.

    b   In the *Conferences* list pane, click the conference you want to paste the copied/cut participant into.

    c   Right-click, and in the drop-down menu select **Paste Participant**.
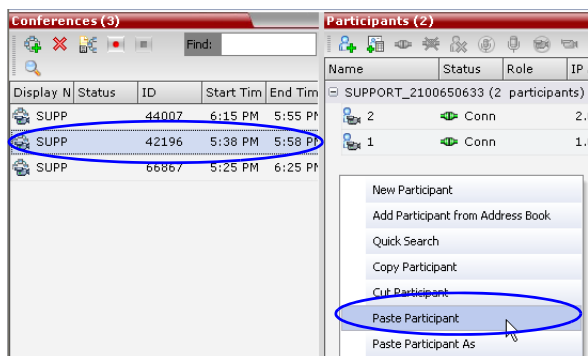
    The participant is connected to the conference.

Paste Participant As

The **Paste Participant As** command allows the *RMX* user to create a new participant using the copied participant's properties as a template. It automatically opens the *Address Book - Participant Properties* dialog box allowing the *RMX* user to modify the participant's properties effectively creating a new participant. When the **OK** button in the *Participant Properties* dialog box is clicked the new participant is connected to the selected conference.

To paste a participant as a new participant:

1   In the *Conferences List* pane, click the conference you want to paste the copied/cut participant into.

    Right-click in the *Participants List* pane of the selected conference and in the drop-down menu select **Paste Participant As**.

    or

    If you are using the *RMX Manager* and you want to paste the participant to a conference on another *RMX*:

    a   In the *MCUs* list pane, click the *RMX* that is hosting the conference that is to receive the participant.

> **b** In the *Conferences* list pane, click the conference you want to paste the copied/cut participant into.
>
> **c** Right-click, and in the drop-down menu select **Paste Participant As**.
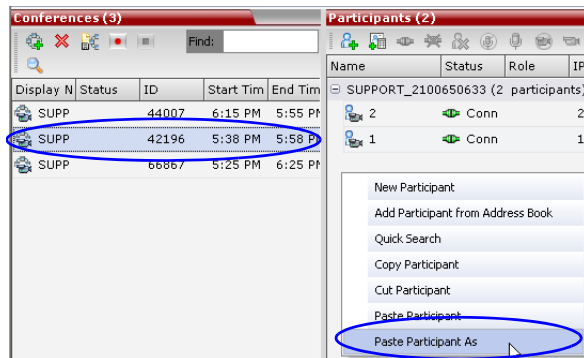
The *Address Book - Participant Properties* dialog box is displayed.
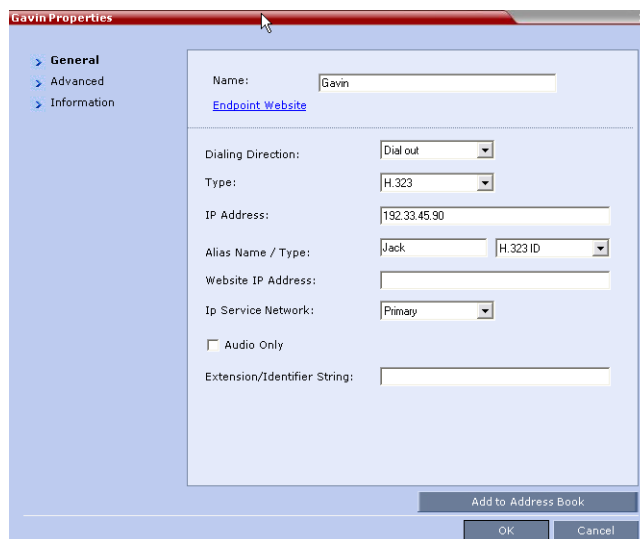
2 Modify the participant information as required. For more information see the *RMX 1500/2000/4000 Administrator's Guide, "Modifying Participants in the Address Book"* on page **5-11**.

Optional. If not already in the *Address Book*, the copied/cut participant can be added to the *Address Book.*

Optional. The new participant can be added to the *Address Book.*

3 Click the **OK** button to connect the new participant to the selected conference.

Copy and Paste Conference

The *RMX* user can **Copy**, and **Paste** conferences. When using the *RMX Web Client*, conferences can copied and pasted on the same *RMX*, however when using the *RMX Manager*, with its ability to manage multiple *RMX*s, conferences can be copied and pasted between different *RMX*s.

Copy Conference

The **Copy** command copies all the conference's properties including connected participants and makes these properties available for pasting, starting a new conference. The copied conference remains active until it terminates or is deleted.

To copy a conference:

1 In the *Conferences List* pane, right-click the conference you want to copy.

2 In the drop-down menu select **Copy Conference**.
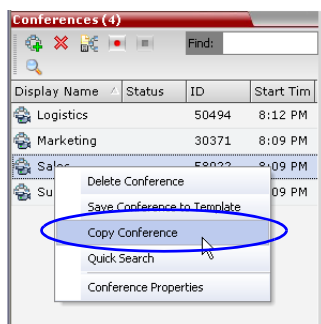
Paste Conference

The **Paste Conference** command starts the new conference on the same *RMX* or on a different *RMX*.

To paste a conference:

>> Right-click in the *Conferences List* pane and in the drop-down menu select **Paste Conference**.

    or

If you are using the *RMX Manager* and you want to paste the conference to a different *RMX*:

a In the *MCUs* list pane, click the *RMX* that is to receive the conference.

b In the *Conferences* list pane, right-click, and in the drop-down menu select **Paste Conference.**
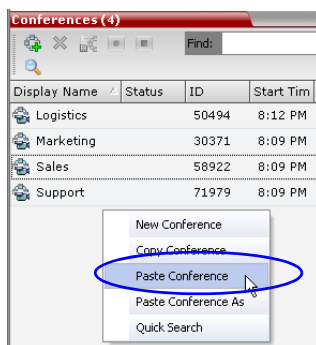
The conference is pasted to the *RMX*.

Paste Conference As

The **Paste Conference As** command allows the *RMX* user to create a new conference using the copied conference's properties as a template. It automatically opens the *Conference Properties* dialog box allowing the *RMX* user to modify the *General*, *Participants* and *Information* tabs to create the new conference. When the **OK** button in the *Conference Properties* dialog box *conference Properties* dialog box is clicked the new conference is started.

To paste a conference as a new conference:

1 Right-click in the *Conferences List* pane and in the drop-down menu select **Paste Conference As**.

   or

   If you are using the *RMX Manager* and you want to paste the conference to a different *RMX*:

   a In the *MCUs* list pane, click the *RMX* that is to receive the conference.

   b In the *Conferences* list pane, right-click, and in the drop-down menu select **Paste Conference As**.
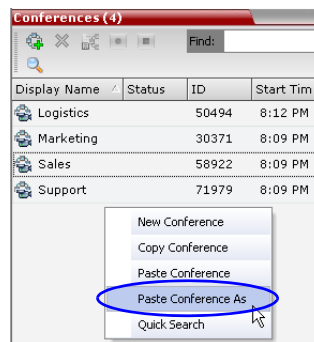
The *Conference Properties* dialog box is displayed.
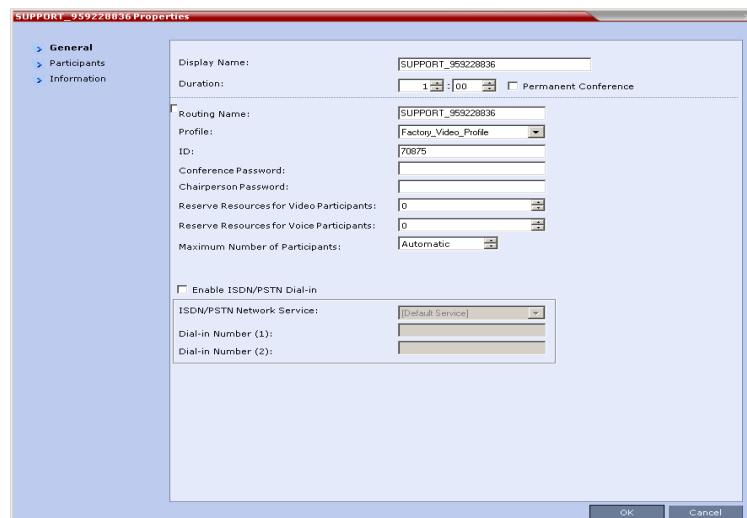
2 Modify the conference information as required.

3 Click the **OK** button to paste and start the new conference.

Resolution Configuration

In previous versions, video resolutions for participants were determined according to a predefined video resolution decision matrix. The decision matrix matched video resolutions to connection line rates, with the aim of providing the best balance between resource usage and video quality at any given line rate.

Version 7.0

The *Resolution Configuration* dialog box enabled the *RMX* administrator to override the default video resolution decision matrix, effectively creating his/her own decision matrix. The minimum threshold line rates at which endpoints are connected at the various video resolutions could be optimized by adjusting the resolution sliders.

Version 7.0.1

Version 7.0.1 incorporated *System Flags* allowing the administrator to modify the minimum bit rate thresholds to prevent potential video quality issues when using endpoints that do not support *H.264 High Profile*.

For more information see "*Flags used in Version 7.0.1*" on page **69**.

Version 7.0.2

Version 7.0.2 incorporates these *System Flags* into a *Resolution Configuration* dialog box designed to enable the administrator to modify the minimum bit rate thresholds to prevent potential video quality issues when using endpoints that do not support *H.264 High Profile*.

Card Configuration Mode

Version 7.0.2 displays the *Resolution Configuration* dialog box according to the *Card Configuration Mode* of the *RMX: MPM+* or *MPMx*.

Guidelines

- *Resolution Slider* settings affect all *Continuous Presence* (*CP*) conferences running on the *RMX*. *Video Switched* conferences are not affected.
- A system restart is not needed after changing the *Resolution Slider* settings.
- *Resolution Slider* settings cannot be changed if there are ongoing conferences running on the RMX.
- The displayed sliders and the resolutions change according the *Card Configuration Mode: MPM+* or *MPMx*.

- The video resolution transmitted to any endpoint is determined by the endpoint's capabilities, the conference line rate, the Conference Profile's Motion and Sharpness settings and the RMX's Card Configuration Mode (MPM+ or MPMx).
- The frames per second (fps) values listed for the video resolutions above are the maximum possible and may be adjusted downward depending on available bandwidth.

Accessing the Resolution Configuration dialog box

The *Resolution Configuration* dialog box is accessed by clicking **Setup > Resolution Configuration** in the *RMX Setup* menu.

The *Resolution Configuration* dialog box display changes according to the *Card Configuration Mode*:

- *MPM+*
- *MPMx* - supports *H.264 High Profile*

Modifying the Resolution Configuration in MPM+ Card Configuration Mode

The *Resolution Configuration* dialog box shown below is displayed when the *RMX* is in *MPM+ Card Configuration Mode*.

The *Resolution Configuration dialog* box opens. It contains the following elements:

- *Max Resolution Pane*
- *Resolution Configuration Pane*
- *Sharpness Resolution Sliders*
- *Motion Resolution Sliders*

Max Resolution   Resolution Configuration

Sharpness
Sliders

Motion
Sliders

Resolutions (Resources per connection)   Selected Minimum Threshold Line Rate for Resolution
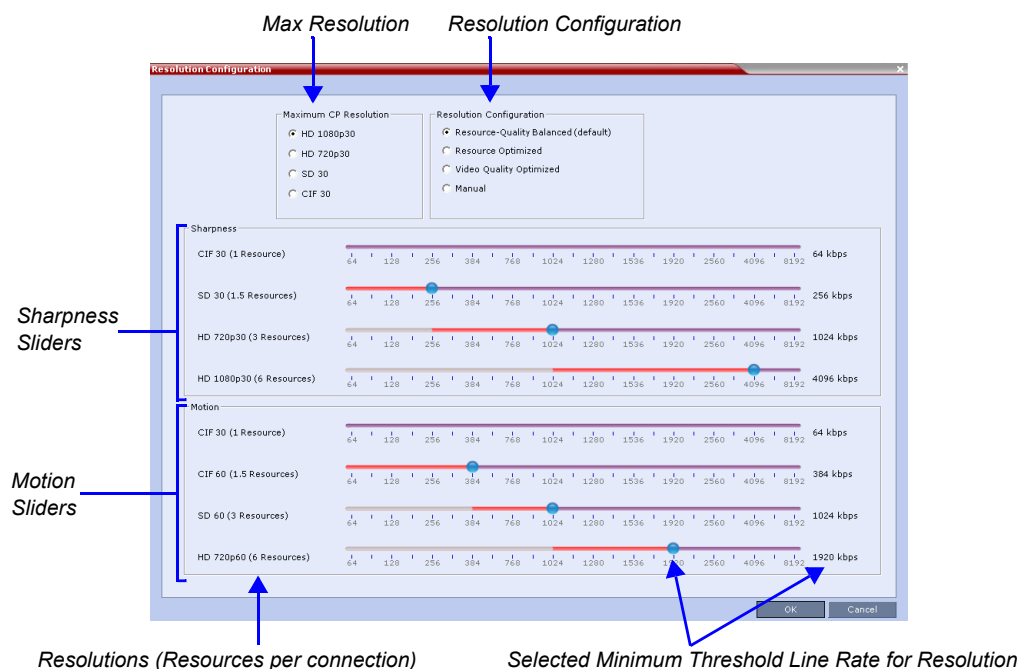
Max Resolution Pane

The *Maximum CP Resolution* of the *RMX* can be set to one of the following resolutions:

- HD 1080p30
- HD 720p30
- SD 30
- CIF 30

Limiting Maximum Resolution

Before a selection is made in this pane, the *Maximum CP Resolution* of the system is determined by the **MAX_CP_RESOLUTION** System Flag.

The **MAX_CP_RESOLUTION** flag value is applied to the system during *First Time Power-on* and after a system upgrade. The default value is *HD1080*.

All subsequent changes to the *Maximum CP Resolution* of the system are made by selections in this pane.

Maximum Resolution

Maximum Resolution can be limited per **conference** or per **participant endpoint**.

131

The *Maximum Conference Resolution,* can be limited via the *Profile - Video Quality* dialog box. For more information see the *RMX 1500/2000/4000 Administrator's Guide "Defining Profiles"* on page **1-9**.

The *Maximum Resolution* can further be limited per participant endpoint via the *Participant - Properties* dialog box. For more information see the *RMX 1500/2000/4000 Administrator's Guide "Adding a Participant to the Address Book"* on page **6-4**.

Resolution Configuration Pane

The user can select from 3 pre-defined *Resolution Configurations* or select a manual *Resolution Slider* adjustment mode. The pre-defined settings can be accepted without modification or be used as the basis for manual fine tuning of resolution settings by the administrator.

The *Manual* radio button is automatically selected if any changes are made to the *Resolution Sliders*.

The *Resolution Configurations* are:

- **Resource-Quality Balanced (default)**

  A balance between the optimized video quality and optimized resource usage. This is the only available resolution configuration in version 6.0.x and earlier.

Use this option:
- When the priority is to maintain a balance between resource usage and video quality.
- When it is necessary to maintain backward compatibility with previous versions.
- When working with CMA.

  The *Balanced* settings are described in the *RMX 1500/2000/4000 Administrator's Guide, "Continuous Presence (CP) Conferencing"* on page **2-3**.

- **Resource Optimized**

  System resource usage is optimized by allowing high resolution connections only at high line rates and may result in lower video resolutions (in comparison to other resolution configurations) for some line rates.

Use this option when the priority is to save MCU resources and increase the number of participant connections.

- **Video Quality Optimized**

  Video is optimized through higher resolution connections at lower line rates increasing the resource usage at lower line rates. This may decrease the number of participant connections.

Use this option when the priority is to use higher video resolutions while decreasing the number of participant connections.

- **Manual**

  The administrator adjusts the sliders to accommodate local conferencing requirements.

Sharpness and Motion Resolution Slider Panes

Sharpness and *Motion* are *Video Quality* settings that are selected per conference and are defined in the conference *Profile* and they determine the resolution matrix that will be applied globally to all conferences according to the selection of *Sharpness* or *Motion*.

The resolution matrix for *Sharpness* or *Motion* is determined by the resolution configuration and can be viewed in the *Resolution Configuration* sliders.

System Resource usage is affected by the *Resolution Configuration* settings.

Example

As shown in following diagram:

- Moving the *HD720p30* resolution slider from 1024kbps to 1920kbps increases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 1024kbps and 1920kbps that would have connected at *HD 720p30* resolution will instead connect at *SD 30* resolution. Each of the affected endpoints will connect at lower resolution but will use 1.5 system resources instead of 3 system resources.

- Moving the *HD1080p30* resolution slider from 4096kbps to 2560kbps decreases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 2560kbps and 4096kbps that would have connected at *HD 720p30* resolution will instead connect at *HD 1080p30* resolution. Each of the affected endpoints will connect at higher resolution but will use 6 system resources instead of 3 system resources.

Modifying the Resolution Configuration in MPMx Card Configuration Mode

The *Resolution Configuration - Basic Configuration* dialog box is the first dialog box displayed when the *RMX* is in *MPMx Card Configuration Mode.*

Clicking the **Detailed Configuration** button toggles the display of the *Detailed Configuration* pane, which displays sliders for modifying minimum connection threshold line rates for endpoints that support *H.264 Base Profile* or *High Profile.* The *Detailed Configuration* pane can also be opened by clicking the **Manual** radio button in the *Resolution Configuration* pane.

Sharpness and *Motion* settings are accessed by clicking the **Sharpness** and **Motion** tabs when the *Detailed Configuration* is open.

Basic Configuration

Detailed Configuration

Sharpness / Motion

Minimum Connection Threshold Line Rate Sliders
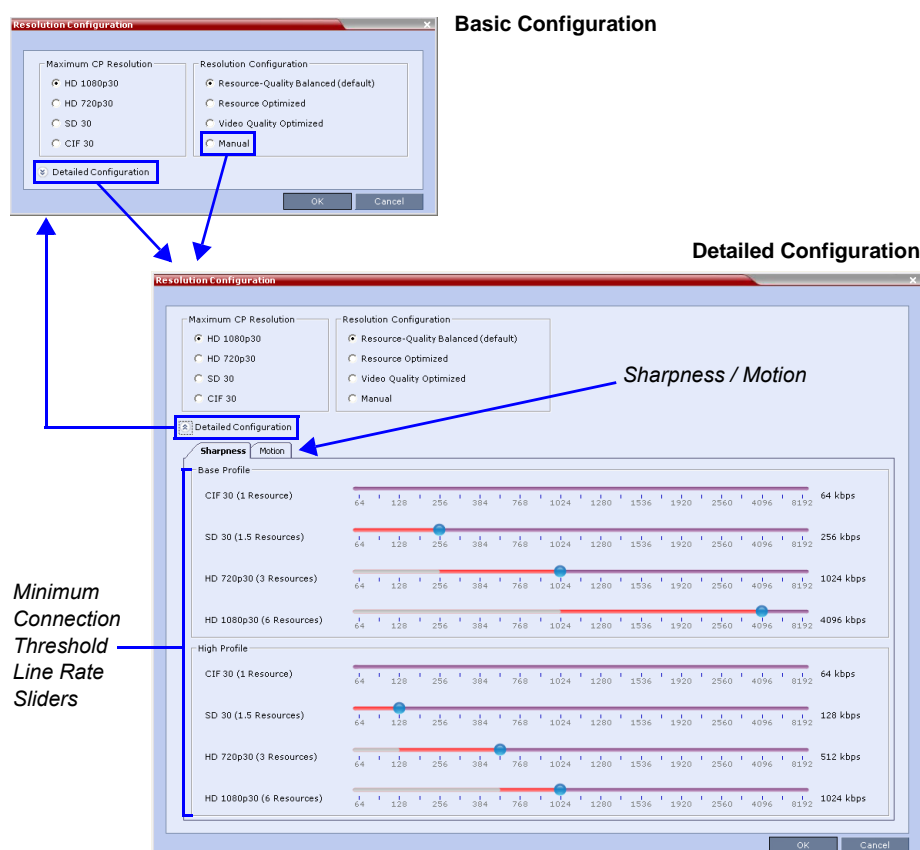
Sharpness and Motion

Sharpness and *Motion* are *Video Quality* settings that are selected per conference and are defined in the conference *Profile.* A conference that has *Sharpness* selected in its *Profile* uses the *Sharpness* settings of the *Resolution Configuration* and likewise a conference that has *Motion* selected in its *Profile* uses the *Motion* settings of the *Resolution Configuration* dialog box.

The *Sharpness* and *Motion* tabs in the *Resolution Configuration* dialog box allow the user to view and modify *Resolution Configuration* settings for conferences with either *Video Quality* setting.

Resolution Configuration - Basic

The *Resolution Configuration -Basic* dialog box contains the following panes:

- *Max CP Resolution Pane*
- *Resolution Configuration Pane*
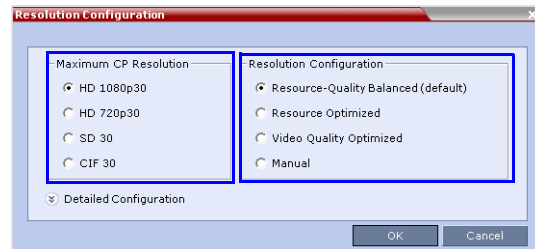
Max CP Resolution Pane

When in *MPMx Card Configuration Mode* the *RMX* can be set to one of the following *Maximum CP Resolutions*:

- HD 1080p30
- HD 720p30
- SD 30
- CIF 30

Limiting Maximum Resolution

Before a selection is made in this pane, the *Maximum CP Resolution* of the system is determined by the **MAX_CP_RESOLUTION** *System Flag*.

For more information see "*Limiting Maximum Resolution"* on page **163**.

Resolution Configuration Pane

The *Resolution Configuration* pane and it's selection options in *MPMx Card Configuration Mode* behave in the same manner as for *MPM+ Card Configuration Mode* as described in the *"Resolution Configuration Pane"* section on page **164**.

Resolution Configuration - Detailed

H.264 High Profile allows higher quality video to be transmitted at lower bit rates.

However, setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile.* The *RMX* uses two decision matrices (*Base Profile, High Profile)* to enable endpoints to connect according to their capabilities.

The *Detailed Configuration* dialog box allows the administrator to configure minimum connection threshold bit rates for endpoints that support *H.264 High Profile* and those that do not support *H.264 High Profile* by using the following slider panes:

- *Base Profile* - Endpoints that do not support *H.264 High Profile* connect at these minimum threshold bit rates.
- *High Profile* - Endpoints that support *H.264 High Profile* connect at these minimum threshold bit rates.
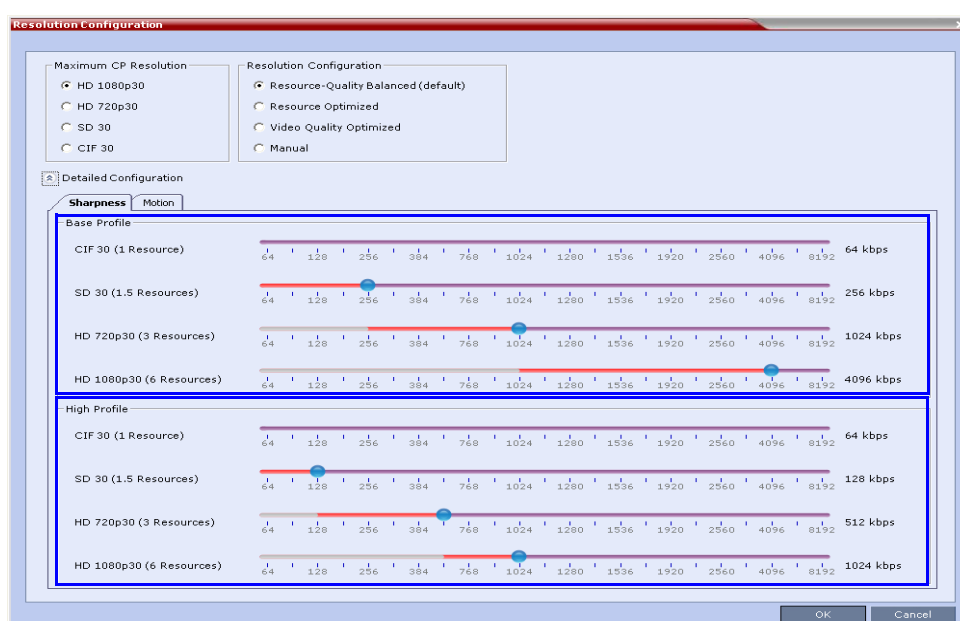
Base Profile / High Profile Resolution Slider Panes

The *Base Profile* and *High Profile* sliders operate in the same manner as that described for the *Sharpness* and *Motion* sliders. For more information see the example in the *"Sharpness and Motion Resolution Slider Panes"* section on page **164**.

Default Minimum Threshold Line Rates

The following Table summarizes the *Default Minimum Threshold Line Rates* and *Video Resource* usage for each of the pre-defined optimization settings for each *Resolution*, *H.264 Profile*, *Video Quality* setting (*Sharpness* and *Motion*) for *MPM, MPM+* and *MPMx Card Configuration Modes*.

			Resource-Quality Balanced (Default)						Resource Optimized						Video Quality Optimized					
			Sharpness			Motion			Sharpness			Motion			Sharpness			Motion		
		Profile	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx
HD1080p30	Default kbps — High	High			1536						4096						1024			
	Base	Base		4096	4096					4096	4096					1728	1728			
	Resources			8	6					8	6					8	6			
HD720p60	Default kbps — High	High						1280						1920					1280	832
	Base	Base					1920	1920					1920	1920					1536	1280
	Resources						8	6					8	6					8	6
HD720p30	Default kbps — High	High			768						1920						512			
	Base	Base	1024	1024	1024				1920	1920	1920				832	832	832			
	Resources		4	4	3				4	4	3				4	4	3			
SD60	Default kbps — High	High						768						1024						768
	Base	Base					1024	1024					1024	1024					512	768
	Resources						4	3					4	3					4	3
SD30	Default kbps — High	High			256						384						256			
	Base	Base	256	256	256				384	384	384				256	256	256			
	Resources		4	2.66	1.5				4	2.66	1.5				4	2.66	1.5			
SD15	Default kbps		256						384						256					
	Resources		2						2						2					
CIF60	Default kbps — High	High						256						384						256
	Base	Base					384	384					384	384					256	256
	Resources						2.66	1.5					2.66	1.5					2.66	1.5
CIF30	Default kbps — High	High			64			64			64			64			64			64
	Base	Base	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64
	Resources		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

(Left vertical axis label: Default Minimum Threshold (kbps) by Resolution, Profile, Resources)

For more information see the *RMX 1500/2000/4000 Administrator's Guide:*

MPM cards are not supported starting with *Version 7.5.0.J.*

High Resolution Slide Enhancements

Conference and *Entry Queue IVR Services* now support customized high resolution slides in addition to the low and high resolution slides included in the default slide set.

Slides can be selected and previewed via the *New Conference* and *New Entry Queue IVR Service* dialog boxes.

Guidelines

- Two customized slides can be loaded per *IVR Service*:
  — A low resolution slide, to be used with low resolution endpoints.
  — A high resolution slide, to be used with high resolution endpoints.
  Table 10 summarizes the recommended input slide formats and the resulting slides that are generated:

Table 10   IVR Slide - Input / Output Formats

Slide Resolution	Format	
	Input Slides	Generated Slides
High	HD1080p (16:9) or HD720p (16:9)	HD1080p HD720p
Low	4CIF (4:3) or CIF (4:3)	4SIF SIF CIF

- The source images for the high resolution slides must be in **.bmp* or **.jpg* format.
- If the uploaded slides are not of the exact *SD* or *HD* resolution, an error message is displayed and the slides are automatically cropped.
- If a slide that is selected in an *IVR Service* is deleted, a warning is displayed listing the *IVR Services* in which it is selected. If deleted, it will be replaced with a default *RMX* slide.
- The generated slides are not deleted if the system is downgraded to a lower software version.
- The first custom source file uploaded, whatever its format, is used to generate both high and low resolution custom slides. High resolution source files uploaded after the first upload will be used to generate and replace high resolution custom slides. Likewise, low resolution source files uploaded after the first upload will be used to generate and replace low resolution custom slides.
- If there are two custom source files in the folder, one high resolution, one low resolution, and a new high resolution custom source file is uploaded, new high resolution custom slides are created. The existing low resolution custom slides are not deleted.
- If there are two custom source files in the folder, one high resolution, one low resolution, and a new low resolution custom source file is uploaded, new low resolution custom slides are created. The existing high resolution custom slides are not deleted.
-

Managing Custom Slides

Custom Slides are managed via the *Video Services* tab of the *New Conference Queue IVR Service* and *New Entry Queue IVR Service* dialog boxes.

Adding, Previewing and Selecting Custom Slides

High Resolution Slides are added, previewed and selected in the same manner as *Low Resolution Slides* were in previous versions.

To upload a *Low Resolution Slide* click the **Add Slide - Low Resolution**.

To upload a *High Resolution Slide* click the **Add Slide - High Resolution**.
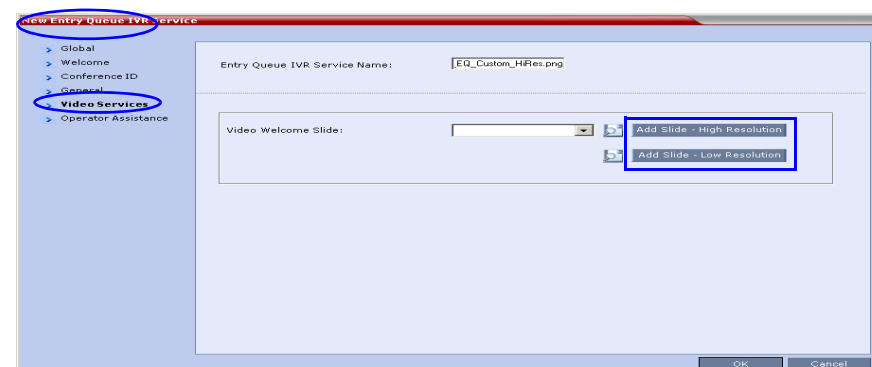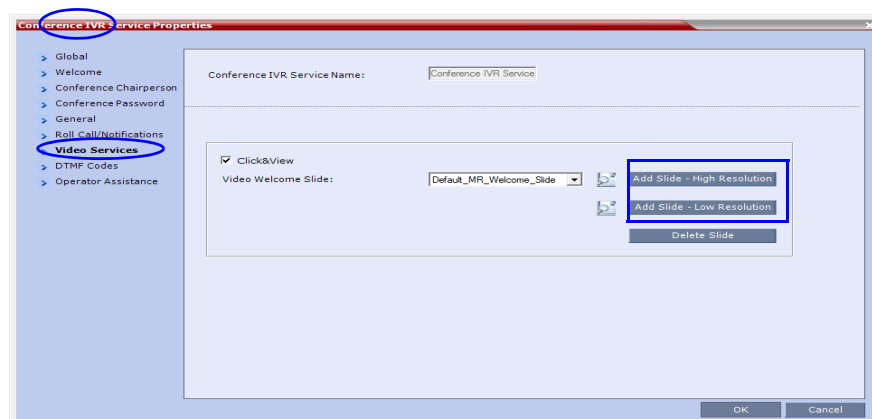
The *Install File* dialog box opens, enabling you to select the required slide.

Once selected, you can Preview the slide.

For more information about *Adding, Previewing* and *Selecting Custom Slides* see the *RMX 1500/2000/4000 Administrator's Guide*, *"Defining a New Conference IVR Service"* on page **15-9** and *"Defining a New Entry Queue IVR Service"* on page **15-31**.

Auto Redial when Endpoint Drops

The *Auto Redialing* option instructs the *RMX* to automatically redial IP and SIP participants that have been abnormally disconnected from the conference.

Guidelines

- The *Auto Redialing* option is disabled by default.
- *Auto Redialing* can be enabled or disabled during an ongoing conference using the *Conference Properties – Advanced* dialog box.
- The *RMX* will not redial an endpoint that has been disconnected from the conference by the participant.
- The *RMX* will not redial an endpoint that has been disconnected or deleted from the conference by an operator or administrator.

Enabling Auto Redialing

Auto Redialing is enabled in the *New Profile – Advanced* or, during an ongoing conference, in the *Profile Properties – Advanced* dialog box.
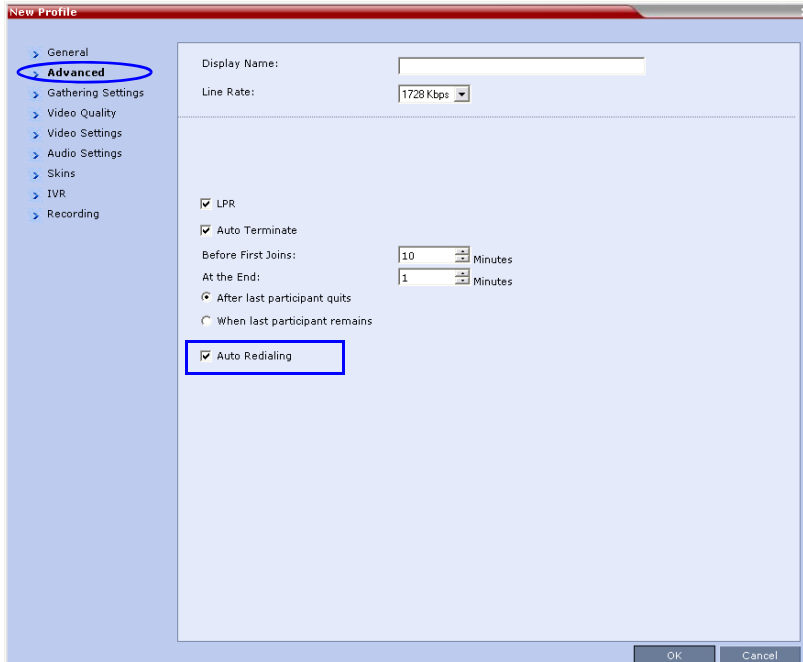
To enable Auto Redialing:.

1   Display the *Conference Profiles* list, and select either the **New Profile** button to create a new Profile or display the **Profile Properties**.

The *New Profile* or *Profile Properties* dialog box is displayed.

2   Click the **Advance** tab.

The *Advanced* tab is displayed.

3   Select the **Auto Redialing** check box.
4   Click the **OK** button.

System Flags

The **ENABLE_IP_REDIAL** *System Flag* is overridden by the *Auto Redialing* setting in the *Conference Profile*.

Auto Redialing is controlled by the two *System Flags* described in Table 11.

If a flag is not listed in the *System Flags* list it must be added to the *system.cfg* file before it can be modified.

To list, modify or add flags to the system.cfg file:

1 In the *RMX Web Client* menu, click **Setup>System Configuration**.

The *System Flags* list is displayed.

2 For each of the flags:

If the flag is listed:

a In the *System Flags* dialog box, click the **Edit Flag** button.

b Enter the *New Value* for the flag.

c Click the **OK** button.

If the flag is not listed:

a In the *System Flags* dialog box, click the **New Flag** button.

b Add the *New Flag* and *Value* as set out in Table 11.

c Click the **OK** button.

Table 11   System Flags – Auto Redialing

New Flag	Description
REDIAL_INTERVAL_IN_SECONDS	Enter the number of seconds that the RMX should wait before successive redialing attempts. Range: 0-30 (Default: 10)
NUMBER_OF_REDIAL	Enter the number redialing attempts required. Dialing may continue until the conference is terminated. Default: 3

3 Click the **OK** button.

Multi-RMX Manager - Import/Export RMX Manager Configuration

The RMX Manager configuration that includes the MCU list and the multilingual selection can be save to any workstation/PC on the network and imported to any Multi-RMX Manager installed in the network. This enables the creation of the MCUs list once and distributing it to all RMX Manager installations on the network.

In addition, when upgrading to a previous version, the MCU list is deleted, and can be imported after upgrade.

The exported file is save in XML format and can be edited in any text editor that can open XML files.

To Export the RMX Manager Configuration:

1   In the Multi-RMX Manager, click the **Export RMX Manager Configuration** button in the toolbar, or right-click anywhere in the MCUs pane and then click **Export RMX Manager Configuration**.
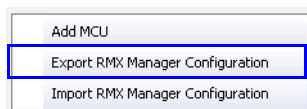
The *Export RMX Manager Configuration* dialog box opens.

2   Click the **Browse** button to select the location of the save file, or enter the required path in the *Export Path* box.
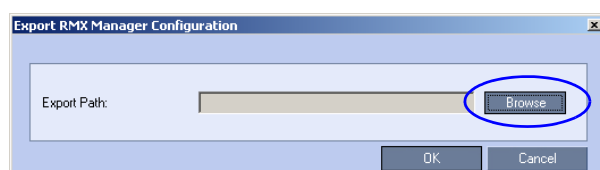
The selected file path is displayed in the *Export Path* box.

3   Click **OK** to export the RMX Manager configuration.

To Import the RMX Manager Configuration:

1   In the Multi-RMX Manager, click the **Import RMX Manager Configuration** button in the toolbar, or right-click anywhere in the MCUs pane and then click **Import RMX Manager Configuration**.
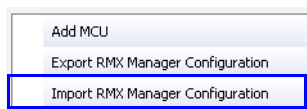
The *Import RMX Manager Configuration* dialog box opens.
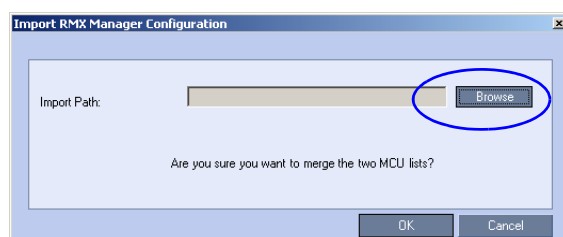
2   Click the **Browse** button to select the saved file, or enter the required path in the *Export Path* box.

The *Open* dialog box is displayed.
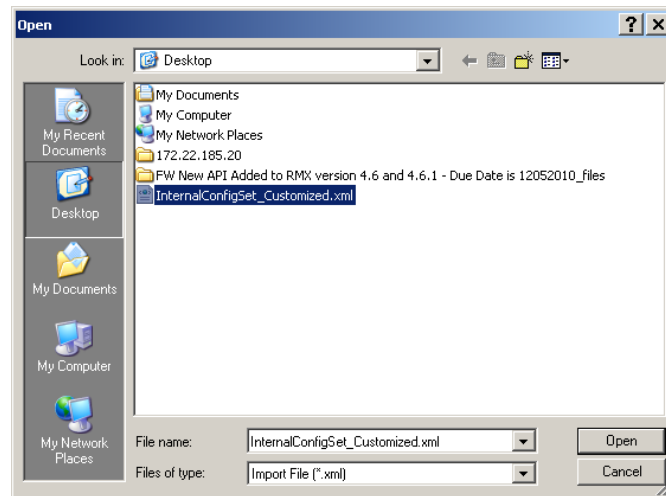
3   Select the XML file previously save, and click the Open button.

The selected file path is displayed in the *Import Path* box.

4   Click **OK** to import the file.

Automatic Password Generation

The RMX can be configured to automatically generate conference and chairperson passwords when the *Conference Password* and *Chairperson Password* fields are left blank.

Guidelines

- If the flag **HIDE_CONFERENCE_PASSWORD** is set to **YES,** the automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags NUMERIC_CONF_PASS_DEFAULT_LEN and NUMERIC_CHAIR_PASS_ DEFAULT _LEN.

- The automatic generation of conference passwords is enabled/disabled by the flag **NUMERIC_CONF_PASS_DEFAULT_LEN**.

- The automatic generation of chairperson passwords is enabled/disabled by the flag **NUMERIC_CHAIR_PASS_ DEFAULT _LEN**.

- The automatically generated passwords will be numeric and random.

- The passwords are automatically assigned to ongoing conferences, Meeting Rooms and Reservations at the end of the creation process (once they are added to the RMX).

- Automatically assigned passwords can be manually changed through the *Conference/Meeting Room/Reservation Properties* dialog boxes.

- Deleting an automatically created password will not cause the system to generate a new password and the new password must be added manually or the field can be left blank.

- If a password was assigned to the conference via Microsoft Outlook using the PCO add-in, the system does not change these passwords and additional passwords will not be generated (for example, if only the conference password was assigned a chairperson password will not be assigned).

- If the flag values (i.e. the password lengths) are changed, passwords that were already assigned to conferences, Meeting Rooms and Reservations will not change and they can be activated using the existing passwords. Only new conferencing entities will be affected by the change.

> Do not enable this option in an environment that includes a Polycom DMA system.

Enabling the Automatic Generation of Passwords

To enable the automatic generation of passwords, the following flags have to be defined:

Table 1-1   *Automatic Password Generation Flags*

Flag	Description
HIDE_CONFERENCE_PASSWORD	**NO (default)** - Conference and chairperson passwords are displayed when viewing the Conference/ Meeting Room/ Reservation properties. It also enables the automatic generation of passwords in general. **Yes** - Conference and Chairperson Passwords are hidden (they are replaced by asterisks). It also disables the automatic generation of passwords.
NUMERIC_CONF_PASS_MIN_LEN	Enter the minimum number of characters required for conference passwords. Possible values: **0 – 16**. **0 (default in non-secured mode)** means no minimum length. However this setting cannot be applied when the RMX is in *Enhanced Security Mode*. **9 (default in Enhanced Security Mode)** Conference password must be at least 9 characters in length.
NUMERIC_CHAIR_PASS_MIN_LEN	Enter the minimum number of characters required for chairperson passwords. Possible values: **0 – 16**. **0 (default in non-secured mode)** means no minimum length. However this setting cannot be applied when the RMX is in *Enhanced Security Mode*. **9 (default in Enhanced Security Mode)**, Chairperson password must be at least 9 characters in length.
NUMERIC_CONF_PASS_MAX_LEN	Enter the maximum number of characters permitted for conference passwords. Possible values: **0 – 16** (non-secured mode) or **9 – 16** (Enhanced Security Mode). **16 (default)** - Conference password maximum length is 16 characters.

145

Table 1-1   *Automatic Password Generation Flags (Continued)*

Flag	Description
NUMERIC_CHAIR_PASS_MAX_LEN	Enter the maximum number of characters permitted for chairperson passwords. Possible values: **0 – 16** (non-secured mode) or **9 – 16** (Enhanced Security Mode). **16 (default)** - chairperson password maximum length is 16 characters.
NUMERIC_CONF_PASS_DEFAULT_ LEN	This flag enables or disables the automatic generation of conference passwords. The length of the automatically generated passwords is determined by the flag value. Possible values: • **0 – 16, 6 default** (non-secured mode) • **0 and 9 – 16, 9 default** (Enhanced Security Mode). Enter **0** to disable the automatic generation of passwords. Any value other than 0 enables the automatic generation of conference passwords provided the flag *HIDE_CONFERENCE_PASSWORD is set to NO.* If the default is used, in non-secured mode the system will automatically generate conference passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_ DEFAULT _LEN	This flag enables or disables the automatic generation of chairperson passwords. The length of the automatically generated passwords is determined by the flag value. Possible values: • **0 – 16, 6 default** (non-secured mode) • **0 and 9 – 16, 9 default** (Enhanced Security Mode). Enter **0** to disable the automatic generation of passwords. Any value other than 0 enables the automatic generation of chairperson passwords provided the flag *HIDE_CONFERENCE_PASSWORD is set to NO.* If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.

If the default password length defined by the *NUMERIC_CONF_PASS_DEFAULT_LEN* or *NUMERIC_CHAIR_PASS_ DEFAULT LEN* does not fall within the range defined by the minimum and maximum length an appropriate fault is added to the Faults list.

IVR Provider Entry Queue (Shared Number Dialing)

In an environment that includes a DMA, the RMX Entry Queue can be configured to provide the IVR Services on behalf of the DMA to SIP endpoints. It displays the Welcome Slide, plays the welcome message and retrieves the destination conference ID that is entered by the participant using DTMF codes.

To enable this feature, a special Entry Queue that is defined as *IVR Service Provider only* is created. This Entry Queue does not forward calls to conferences running on the RMX and its main functionality is to provide IVR services.

Call Flow

The SIP participant dials the DMA Virtual Entry Queue number, for example 1000@dma.polycom.com.

The DMA forwards the SIP call to the RMX, to a special Entry Queue that is configured as *IVR Service Provider Only*. The participant is prompted to enter the conference ID using DTMF codes.

Once the participant enters the conference ID, the conference ID is forwarded to the DMA, enabling the DMA to connect the SIP endpoint to the destination conference or create a new conference and connect the participant to that conference.

Guidelines

- An Entry Queue defined as IVR service provider only does not route the SIP call to a target conference and it cannot be used to rout calls on the RMX. In such a configuration, the DMA handles the calls. Therefore, normal Entry Queues must be defined separately.
- *Operator Assistance* must be disabled in the IVR Service assigned to this Entry Queue.
- Only the conference ID prompts should be configured. Other prompts are not supported in *IVR Service Provider Only* configuration.
- PSTN, ISDN, H.323 calls to this Entry Queue are rejected.
- The DMA must be configured to locate the *IVR Service Provider Only* Entry Queue on the RMX. To locate the Entry Queue the DMA requires the Entry Queue's ID number and the RMX Central Signaling IP address (xxx.xx.xxx.xx).
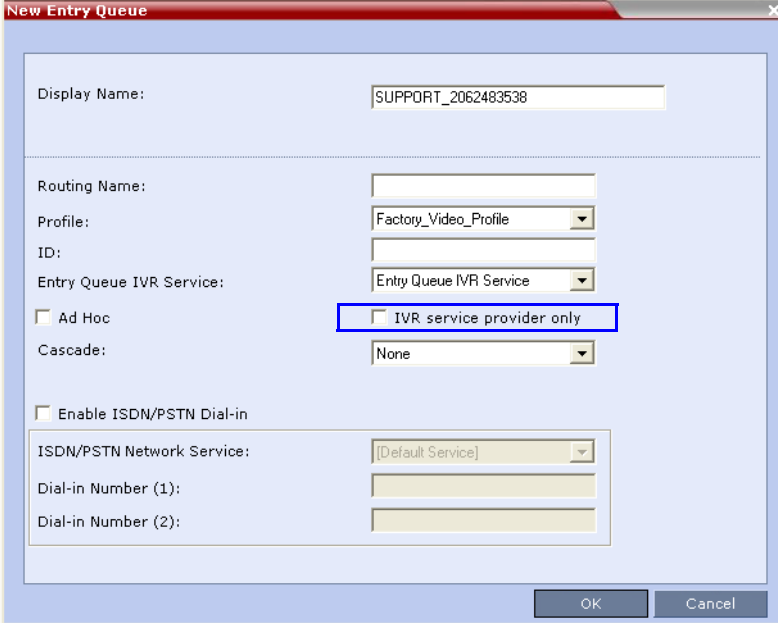
RMX Configuration

Entry Queue IVR Service

If required, create a special Entry Queue IVR Service in which the *Operator Assistance* option is disabled and only the *Conference ID* prompts are enabled.

Entry Queue

>> In the *New Entry Queue* dialog box, select **IVR Service Provider Only.**

— Enter the Entry Queue ID that will be used by the DMA to forward the SIP calls to this Entry Queue.

— Select the special Entry Queue IVR Service if one was created.

— *Ad Hoc*, *Cascade* and *Enable ISDN/PSTN Dial-in* options should not be selected with this type of Entry Queue.

Detailed Description - Changes to Existing Features

The following table lists the changes to existing features in Version 7.5.0.J.

Table 2   *Feature Changes List*

	Category	Feature Name	Description
5	General	Resolution Sliders	
6	General	System Configuration Flag	
7	General	System Configuration Flag	
8	General	System Configuration Flag	

RMX Resource Management by CMA and DMA

Currently, when both *CMA* and *DMA* are part of the solution, each application works independently and is unaware of the RMX resources used by the other application.

In this version, following a request by the CMA and DMA, the RMX will send updates on resource usage to both *CMA* and *DMA,* with each application updating its own resource usage for the RMX. This provides better management of the RMX resources by CMA and DMA.

Guidelines

- Resource usage updates from RMX to the CMA and DMA are supported only with RMXs with MPM+ Cards.
- Both Flexible Resource Capacity™ and Fixed Resource Capacity™ modes are supported.
- Following requests sent by CMA and DMA, the RMX will send the number of occupied resources for a conference or total for the MCU, according the Resource capacity mode used by the system.
  - In *Flexible Resource Capacity Mode*, *CMA/DMA* receive information about how many *Video* (*CIF*) and *Audio* resources are occupied per conference or MCU according the request type sent by the CMA and DMA.
  - In *Fixed Resource Capacity™ Mode*, *CMA/DMA* receive information about the number of occupied resources per resource type (Audio only, CIF, SD, HD 720p, HD 1080p) and per conference or MCU according the request type sent by the CMA and DMA.
- Occupied resources are resources that are connected to ongoing conferences. Disconnected endpoints in an ongoing conference are not counted as occupied resources.
- An ongoing conference that does not include participants and the *Send Content to Legacy Endpoints* option is disabled does not occupy resources. If the *Send Content to Legacy Endpoints* option is enabled, the conference occupies one SD resource.
- The RMX is unaware of the resource usage split between the CMA and DMA.

Immersive Telepresence (ITP) Enhancements

Changes to the New Profile Dialog Box

The *New Profile - Video Settings* dialog box has been modified to enable enhanced control of *ITP* features such as:

- Automatic detection of *ITP* sites.
- Retrieval of *Telepresence Layout Mode.*
- *Layout* control.
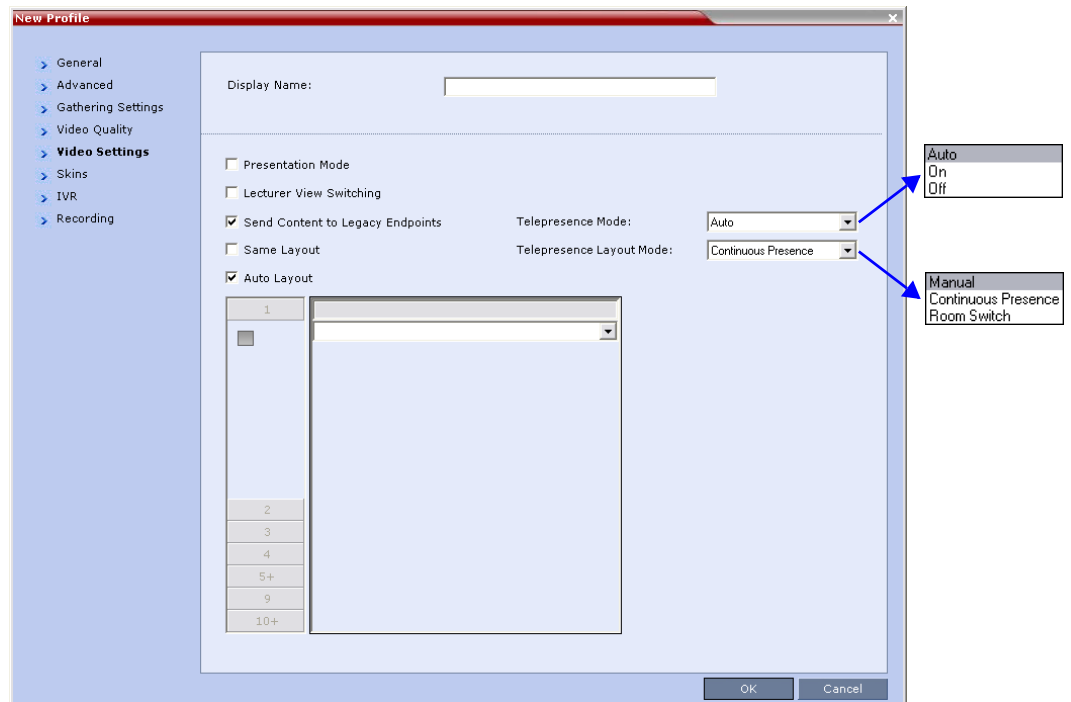
> The Telepresence *Mode* and *Telepresence Layout Mode* fields are only displayed if the *RMX* has a Telepresence license installed.

Automatic detection of Immersive Telepresence (ITP) Sites

A *Telepresence Mode* drop-down menu replaces the previous check box in the *New Profile – Video Settings* dialog box containing the following options:

- Off
- Auto (Default)
- On

ITP endpoints are automatically detected. If *ITP* endpoints are detected, *ITP* features are applied and the *RMX* sends conference video with the following options disabled:

- Borders
- Site names
- Speaker indication
- Skins
- Same Layout

- Presentation Mode
- Auto Layout
- Lecture Mode

Table 3 summarizes the *Telepresence Mode* options.

Table 3   *Telepresence Mode Options*

Telepresence Mode	Description
OFF	When OFF is selected, normal conference video is sent by the RMX.
AUTO (Default)	When AUTO is selected and any ITP endpoints are detected, ITP features are applied to the conference video for all participants.
	When AUTO is selected, the ITP features are dynamic. If all ITP endpoints disconnect from the conference, normal conference video is resumed for all participants. ITP features are resumed for all participants should an ITP endpoint re-connects to the conference.
ON	ITP features are applied to the conference video for all participants regardless of whether there are *ITP* endpoints connected or not.

Retrieving the Telepresence Layout Mode

A new field, *Telepresence Layout Mode*, has been added to the *New Profile – Video Settings* dialog box, enabling *VNOC* operators and *Polycom Multi Layout Applications* to retrieve *Telepresence Layout Mode* information from the *RMX*.
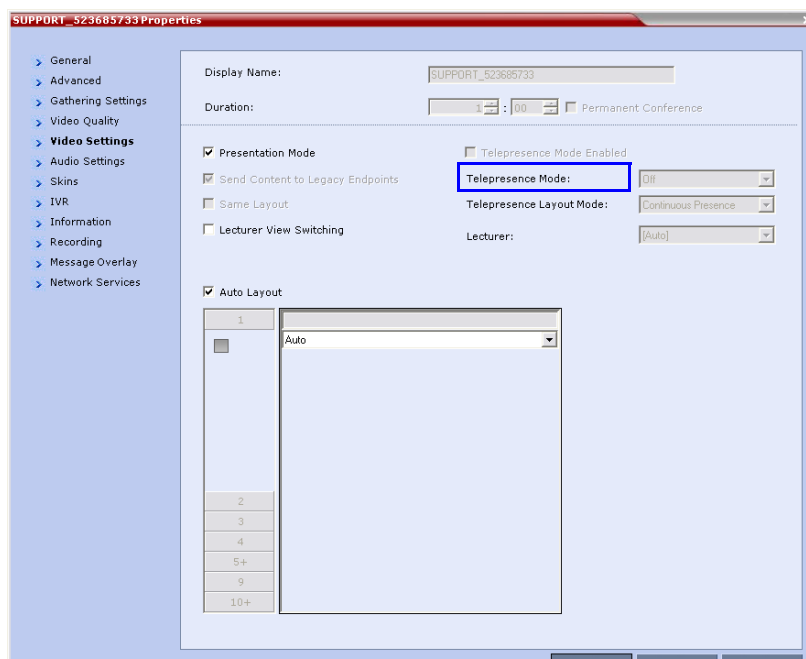
The following modes can be selected:

- *Manual*
- *Continuous presence* - Room Continuous Presence (Default)
- *Room Switch* - Voice Activated Room Switching

Monitoring Telepresence Mode

Monitoring Ongoing Conferences

A additional status indicator, *Telepresence Mode Enabled*, is displayed in the *Conference Properties - Video Settings* tab when monitoring ongoing conferences.
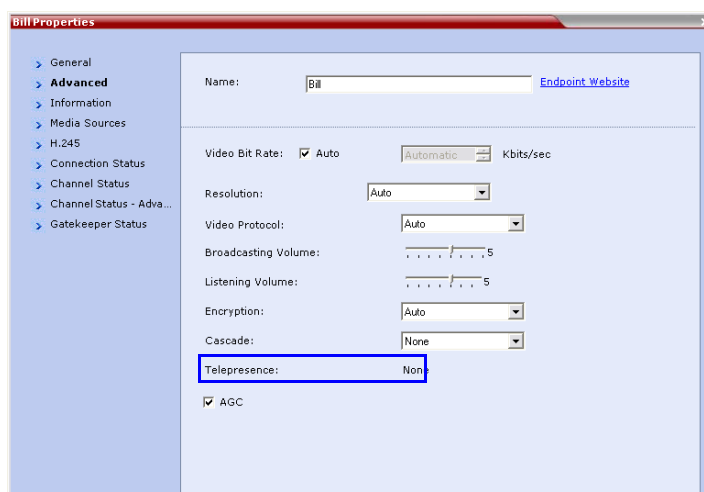
> The Telepresence *Mode Enabled, Telepresence Mode* and *Telepresence Layout Mode* fields are only displayed if the *RMX* has a Telepresence license installed.

If *Telepresence Mode* is enabled, a check mark is displayed in the check box. The field description and the check box are grayed as this a status indicator and cannot be used to enable or disable *Telepresence Mode*.

Monitoring Participant Properties

A additional status indicator, *Telepresence*, is displayed in the *Participant Properties - Advanced* tab when monitoring conference participants.

The *Telepresence* mode of the participant is indicated:

- *RPX* - the participant's endpoint is transmitting 4:3 video format.
- *TPX* - the participant's endpoint is transmitting 16:9 video format.
- *None*.

Striping Options

Horizontal Striping

Horizontal Striping is used by the *RMX* in order to prevent cropping and preserve the aspect ratio of video for all *Telepresence Modes*.
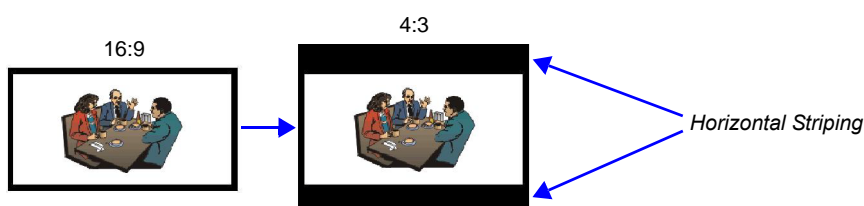
Asymmetric Letter box Cropping

Asymmetric Letter box Cropping is used by the *RMX* in order to preserve the aspect ratio of video for all *Telepresence Modes*.
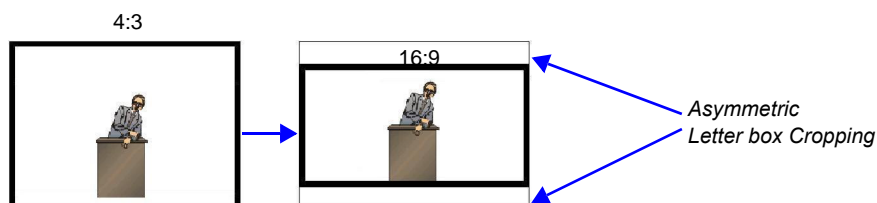
Gathering Phase with ITP Room Systems

When a conference is configured to include a *Gathering Phase*, only one endpoint name is displayed for the *ITP* room in the connected participant list of the *Gathering* slide. The *ITP* room endpoint with the suffix "1" in its name receives the *Gathering* slide.

All layouts available to all participants

In previous versions, additional layouts were available only to *TPX* endpoints. In this version all layouts are available to all endpoints on both conference layout and *Personal Layout* levels.

Aspect ratio for standard endpoints

Standard endpoints (non-*ITP*) receive video from the *RMX* with the same aspect ratio as that which they transmitted to the *RMX*.

Video Fade is enabled for all Telepresence conferences

Video Fade, disabled for *Telepresence* conferences in previous versions, is enabled for all *Telepresence* conferences.

Limiting Maximum Resolution

The *Maximum Resolution* settings of the *Resolution Configuration* dialog box can be overridden by new fields that have been included in the *New Profile* and *New Participant* dialog boxes.

The *Maximum Resolution* field in the *New Profile - Video Quality* dialog box allows *Maximum Resolution* to be limited per conference.

The *Resolution* field in the *New Participant - Advanced* dialog box allows *Maximum Resolution* to be **further limited** per participant endpoint.
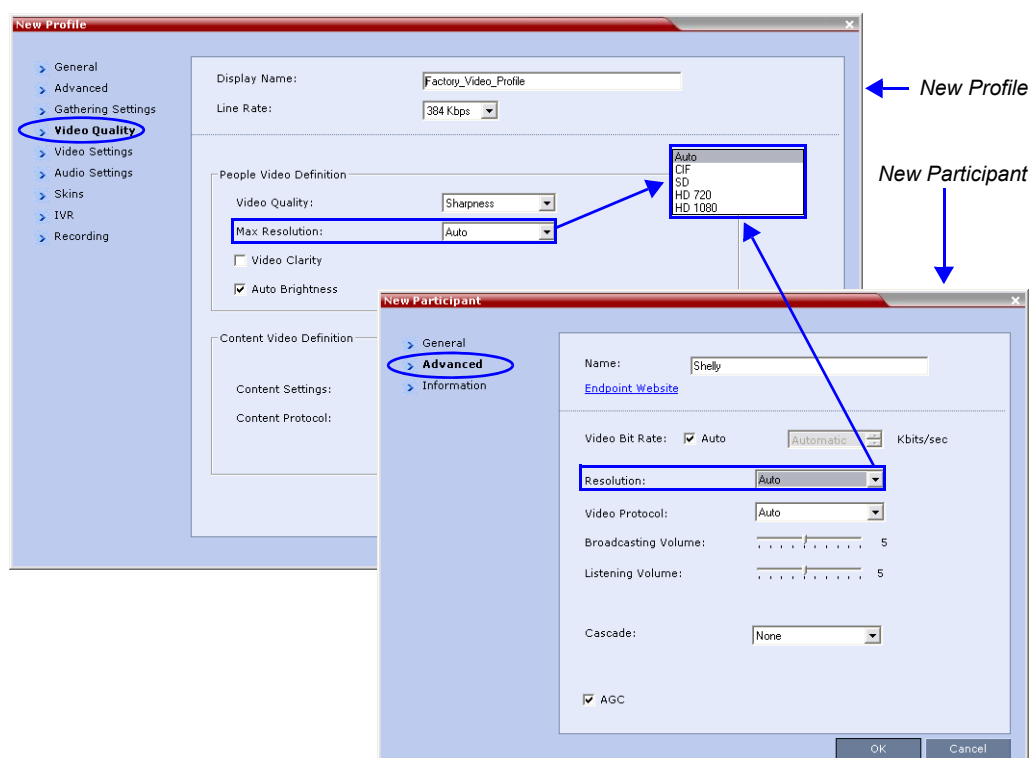
The drop-down menu in both the dialog boxes allow the administrator to select from the following *Maximum Resolution* options:

• *Auto* (default) - The *Maximum Resolution* remains as selected in the Resolution Configuration dialog box.

• *CIF*

• *SD*

• *HD720*

• *HD1080*

The *Maximum Resolution* settings can be monitored in the *Profile Propertie*s - *Video Quality* and *Participant Properties - Advanced* dialog boxes.

The *Maximum Resolution* settings for conferences and participants cannot be changed during an ongoing conference.

For more information see "*Max Resolution Pane"* on page **46**.

Auto Layout Changes

In previous versions, In *Auto Layout* mode, the same video layout (1+7) was displayed when the number of participants was 8 or more.

In this version, two additional layouts are activated in Auto Layout mode when 11 and 12+ participants are connected to the conference. The following table summarizes the default layout selection according to the number of participants connected to the conference:

Table 4   *Auto Layout – Default Layouts*

Number of Video Participants	Auto Layout Default Settings
0-2	
3	
4–5	
6–7	
8-10	
11	
12+	

In layout 2+8, the two central windows display the last two speakers in the conference: the current speaker and the "previous" speaker. To minimize the changes in the layout, when a new speaker is identified the "previous" speaker is replaced by the new speaker while the current speaker remains in his/her window.

Click&View Changes

The video layout options available for 9+ participants has changed.

The following table summarizes the Video Layout options available via *Click&View*.

Table 5   *Video Layout Options*

DTMF Code	Layout Options			
1				
2				
3				
4				

Table 5   *Video Layout Options (Continued)*

DTMF Code	Layout Options				
5	▦	▦	▦		
6	▦				
8	▦				
9	▦	▦	▦	▦	▦

System Configuration - Auto Layout Flags

Two new flags were added to the system configuration file, enabling the configuration of the video layout that will be automatically displayed in Auto Layout mode:

- **PREDEFINED_AUTO_LAYOUT_11**,

  default value: **CP_LAYOUT_2P8** (▦)
- **PREDEFINED_AUTO_LAYOUT_12**,

  default value: **CP_LAYOUT_1P12** (▦)

For more details on Auto Layout flag configuration, see *RMX 1500/2000/4000 Administrator's Guide*, *"Auto Layout Configuration"* on page **19-41**.

Auto Brightness

A new check box, *Auto Brightness,* has been added to the *New Profile - Video Quality* dialog box.

Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.
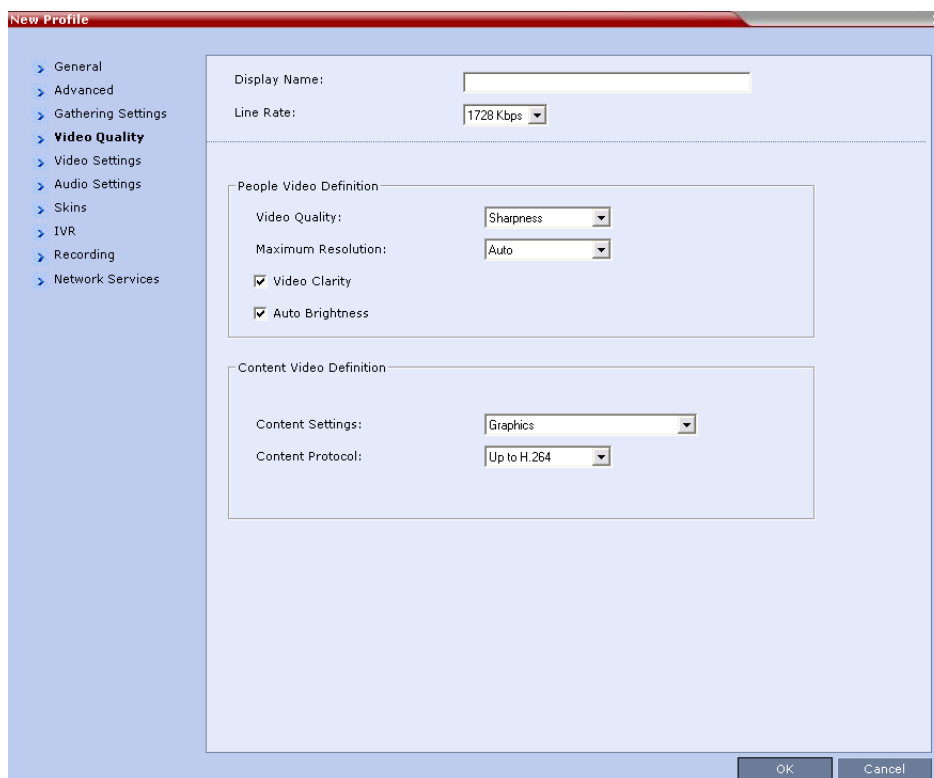
Guidelines

- *Auto Brightness* is supported with *MPM+* and *MPMx* cards only.
- *Auto Brightness* only increases brightness and does not darken video windows.
- *Auto Brightness* is selected by default.
- *Auto Brightness* cannot be selected and deselected during an ongoing conference.

Audio Only Message

In previous versions, participants that were connected as *Secondary* (*Audio Only*)

because of lack of video resources would not receive any indication stating the reason why his/her video had not connected.

In this version, the administrator can enable an audio message that informs the participant of the lack of *Video Resources* in the *RMX* and that he/she is being connected as *Audio Only*. The message states: *All video resources are currently in use. Connecting using audio only.*

Guidelines

- The *IVR* message applies to video participants only. *Audio Only* participants will not receive the message.
- Only *H*.323 and *SIP* participants receive the audio message.
- Downgrade to *Audio Only* is not supported for undefined *ISDN* dial in participants. These participants are disconnected if there is a lack of *Video Resources*.
- The audio message is the first message after the call is connected, preceding all other *IVR* messages.
- The message is called *No Video Resources-Audio Only* and the message file (*.wav*) is called *No video resources audio only.wav*.
- The audio message must be added to the *Conference* and *Entry Queue IVR Services* separately.
- The IVR message can be enabled/disabled by the administrator using the **ENABLE_ NO_VIDEO_RESOURCES_ AUDIO_ONLY_MESSAGE** *System Flag* in *system.cfg*.
  — Possible values: **YES / NO**
  — Default: **YES**

If you wish to modify the flag value, the flag must be added to the *System Configuration* file. For more information see the *RMX 1500/2000/4000 Administrator's Guide, "Modifying System Flags"* on page **19-6**.

Enabling the Audio Only Message

Conference IVR Service

The message file is added to the *Conference IVR Service* according to the procedure described in the *RMX 1500/2000/4000 Administrator's Guide, "Defining a New Conference IVR Service"* on page **15-9**.
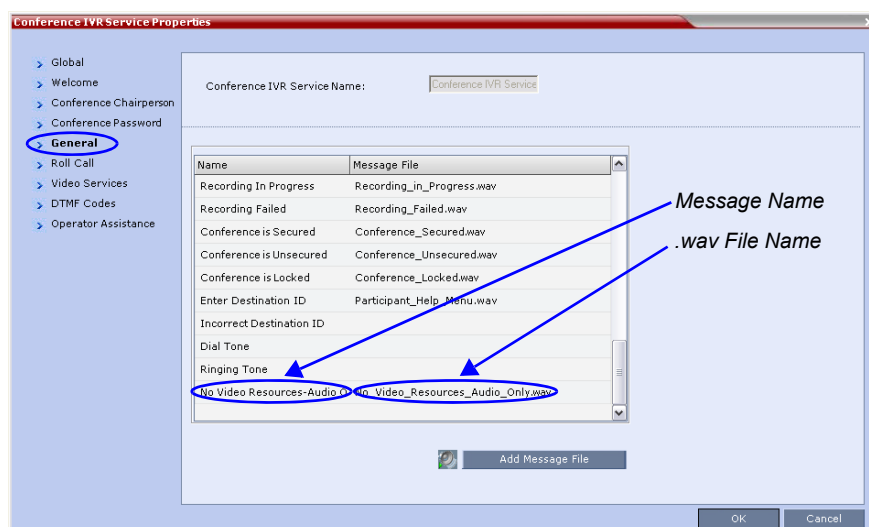
Entry Queue IVR Service

A new dialog box tab, *General*, has been added to the *Entry Queue IVR Service* dialog box. The message name and .wav file name are added to the *Entry Queue IVR Service* in this dialog box. The message file is added to the *Entry Queue IVR Service* in the same manner as described for the *Conference IVR Service* in the *RMX 1500/2000/4000 Administrator's Guide "Defining a New Conference IVR Service"* on page **15-9**.
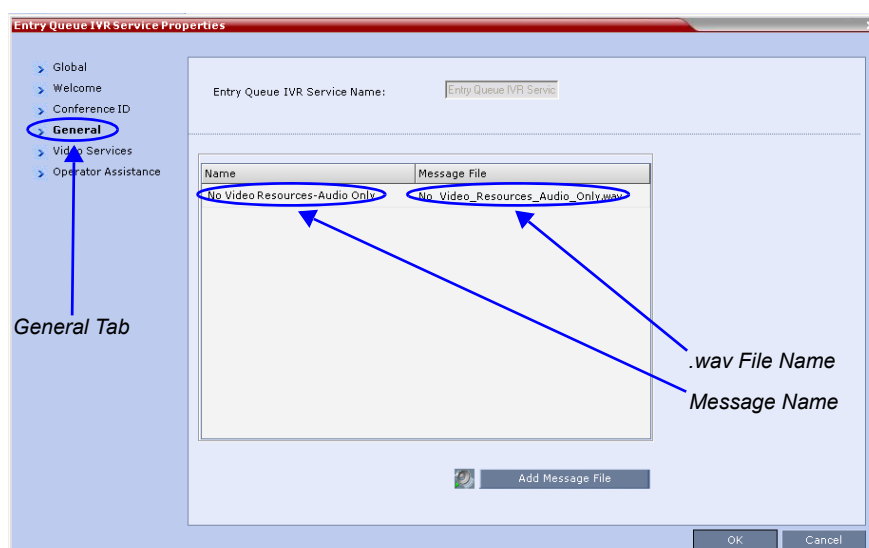
Audio Settings Tab

A new tab, *Audio Settings,* has been added to the *New Profile* dialog box. It contains settings for:

- *Echo Suppression* - moved from the *New Profile - Advanced* tab.
- *Keyboard Noise Suppression* - moved from the *New Profile - Advanced* tab.
- *Audio Clarity:*

  Audio Clarity improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity.

  The enhancement is applied to the following low bandwidth (8kHz) audio algorithms:
  — G.729a
  — G.711

Audio Clarity Guidelines

- *Audio Clarity* is supported with MPM+ and MPMx cards only.
- *Audio Clarity* is selected by default.
- *Audio Clarity* cannot be selected and deselected during an ongoing conference.
- The check box overrides the **SET_AUDIO_CLARITY** *System Flag* in *system.cfg*. For more information see the *RMX 1500/2000/4000 Administrator's Guide, "Defining Profiles"* on page **1-9** and *"Modifying System Flags"* on page **19-6**.
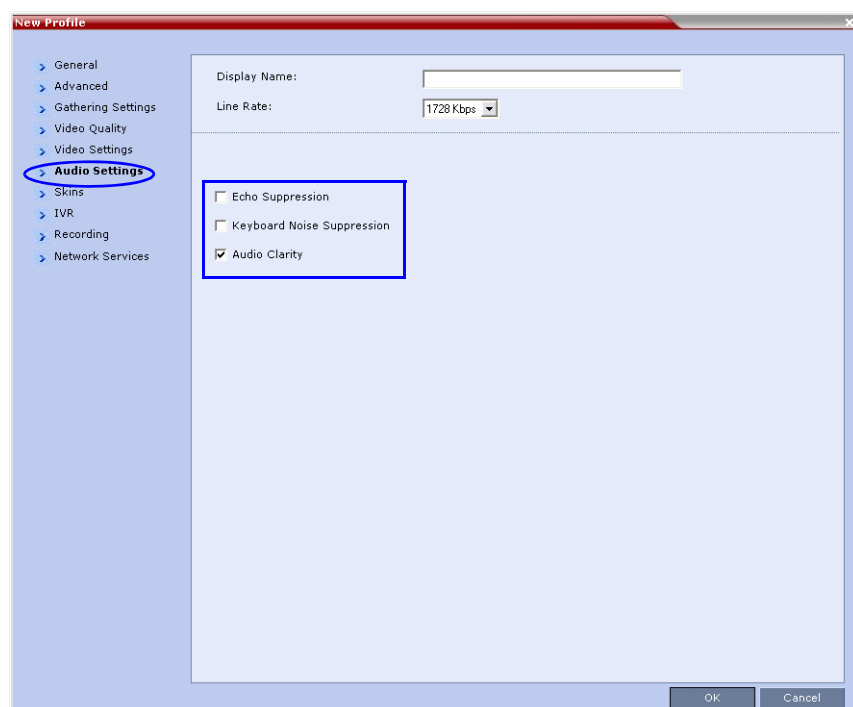
DTMF Forwarding Suppression

Forwarding of the DTMF codes from one conference to another over an ISDN cascading link can be limited to basic operations while suppressing all other operations once the connection between the cascaded conferences is established.

Guidelines

- The forwarding of most of the DTMF codes from one conference to another is available only in cascading between two MCUs.
- When cascading between two RMXs, it is recommended that version 7.0.x is installed on both RMXs to enable the suppression of DTMF code forwarding.
- It is available also when cascading between RMX and MGC.
- RMX can be used as gateway, forwarding the call to the second MCU.
- The following operations are available throughout the conference and the forwarding of their DTMF codes is not suppressed (i.e. they will apply to both conferences):
  — Terminate conference.
  — Mute all but me.
  — Unmute all but me.
  — Secure conference.
  — Unsecure conference.
- The called RMX (RMX B) automatically identifies the calling participant as an MCU and the connection is identified as a cascading link.
- The link (participant) is identified by the same cascading link icon (![icon]) as H.323 link.
- Content sharing is not supported across ISDN Cascading link.

ISDN Cascading is not supported in *Ultra Secure Mode*.

Call Flow and Configuration

ISDN connection can be used to link between two MCUs and create a cascading conference.
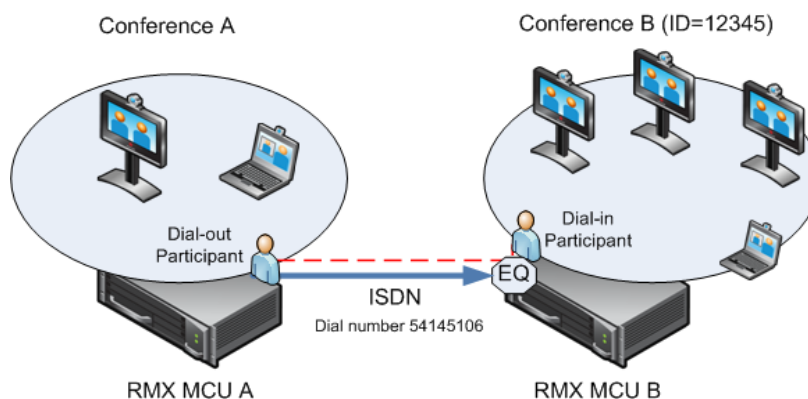
Figure 5   *Cascading Between Two MCUs Using an ISDN Link*

ISDN Network Service is configured in both MCUs. The Entry Queue or conference (for direct dial-in) is enabled for ISDN connection and a dial-in number is assigned (for example 54145106).

A dial out ISDN participant is defined (added) to conference A. The participants's dial out number is the dial-in number of the Entry Queue or conference running on MCU B (for example 54145106).

MCU A dials out to an Entry Queue or conference B running on MCU B using the Entry Queue number (for example 54145106) or the conference number.

When the participant, who is a dial-in participant in conference B, connects to the Entry Queue, the system plays to all the participants in Conference A the IVR message requesting the participant to enter the destination conference ID (or if connecting to a conference directly, the participant is requested to enter the conference password).

At this point the Conference A organizer or any other participant in the conference can enter the required information for the IVR session using DTMF codes. For example, the meeting organizer enters the destination conference ID - 12345.

Any DTMF input from conference A is forwarded to the Entry Queue on MCU B to complete the IVR session and enable the move of the participant to the destination conference B.

Once the DTMF codes are entered and the IVR session is completed, the participant is connected to the conference and the connection between the conferences is established. The system automatically identifies the calling participant as an MCU and the connection is identified as a cascading link and the cascading link icon is displayed for

the participant. ( )

The time period (in seconds) that MCU A will forward DTMF input from conference participants to the second MCU is defined by the system flag **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS**.

Once the timer expires, most of the DTMF codes (excluding five operations) entered in conference A will not be forwarded to conference B. This is done to prevent an operation requested by a participant individually (for example, mute my line) to be applied to all the participants in conference B.

System Flags

The **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS** *System Flag* determines the number of seconds the system waits for DTMF input from the conference participants and forwards them to the second MCU before it will switch to forwarding suppression mode.

Flag range: **0 - 360000**

This flag is defined on MCU A (the calling MCU).

If a flag is not listed in the *System Flags* list it must be added to the *system.cfg* file before it can be modified.

To list, modify or add flags to the system.cfg file:

1   In the *RMX Web Client* menu, click **Setup>System Configuration**.

   The *System Flags* list is displayed.

2   For each of the flag*s*:

   If the flag is listed:

   a   In the *System Flags* dialog box, click the **Edit Flag** button.

   b   Enter the *New Value* for the flag.

   c   Click the **OK** button.

   If the flag is not listed:

   a   In the *System Flags* dialog box, click the **New Flag** button.

   b   Add the *New Flag* name and *Value.*

   c   Click the **OK** button.

3   Click the **OK** button.

Welcome to Polycom® RMX® 1500 / RMX® 2000 / RMX® 4000
(Software Version 7.5.0.J)

END USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE

IMPORTANT-READ CAREFULLY BEFORE USING THE SOFTWARE PRODUCT: This End-User License Agreement ("Agreement") is a legal agreement between you (and/or any company you represent) and either Polycom (Netherlands) B.V. (in Europe, Middle East, and Africa), Polycom Asia Pacific PTE Ltd. (in Asia Pacific), or Polycom, Inc. (in the rest of the world) (each referred to individually and collectively herein as "POLYCOM"), for the SOFTWARE PRODUCT (including any virus or vulnerability updates, and any software updates or upgrades thereto licensed by POLYCOM or its suppliers. The SOFTWARE PRODUCT includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By clicking "I AGREE" or by installing, downloading, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be and will be bound by the terms of this Agreement as a condition of your license. If you do not agree to the terms of this Agreement, your use is prohibited and you may not install or use the SOFTWARE PRODUCT.

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed (not sold) to you, and its use is subject to the terms of this Agreement. This is NOT a sale contract.

1. GRANT OF LICENSE. Subject to the terms of this Agreement, POLYCOM grants to you a non-exclusive, non-transferable (except as set forth herein), revocable license to install and use the SOFTWARE PRODUCT solely on the POLYCOM product with which this SOFTWARE PRODUCT is supplied (the "PRODUCT"). You may use the SOFTWARE PRODUCT only in connection with the use of the PRODUCT subject to the following terms and the proprietary notices, labels or marks on the SOFTWARE PRODUCT or media upon which the SOFTWARE PRODUCT is provided. You are not permitted to lease, rent, distribute or sublicense the SOFTWARE PRODUCT, in whole or in part, or to use the SOFTWARE PRODUCT in a time-sharing, subscription service, hosting or outsourcing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the SOFTWARE PRODUCT (source code). Except as expressly provided below, this License Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights in respect to the SOFTWARE PRODUCT. You are solely responsible for use of the PRODUCT and the SOFTWARE PRODUCT by your agents, contractors, outsourcers, customers and suppliers and their compliance with this Agreement.

2. OTHER RIGHTS AND LIMITATIONS.

2.1   Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, modify or disassemble the SOFTWARE PRODUCT or otherwise reduce the SOFTWARE PRODUCT to human-perceivable form in whole or in part, except and only to the extent that such activity is expressly permitted by a third party license or applicable law, notwithstanding this limitation. The foregoing includes but is not limited to review of data structures or similar materials produced by SOFTWARE PRODUCT. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one PRODUCT. You may not use the SOFTWARE PRODUCT for any illegal purpose or conduct.

2.2   Back-up. Except as expressly provided for under this Agreement you may not copy the SOFTWARE PRODUCT; except, however, you may keep one copy of the SOFTWARE PRODUCT and, if applicable, one copy of any previous version, for back-up purposes, only to be used in the event of failure of the original. All copies of the SOFTWARE PRODUCT must be marked with the proprietary notices provided on the original SOFTWARE PRODUCT. You may not reproduce the supporting documentation accompanying the SOFTWARE PRODUCT.

2.3   No Modifications. You may not modify, translate or create derivative works of the SOFTWARE PRODUCT.

2.4   Proprietary Notices. You may not remove or obscure any proprietary notices, identification, label or trademarks on or in the SOFTWARE PRODUCT or the supporting documentation.

2.5   Software Transfer. You may permanently transfer all of your rights under this Agreement solely in connection with transfer of the PRODUCT, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades or updates, this Agreement, and, if applicable, the Certificate of Authenticity), and the recipient agrees to the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade or update, any transfer must include all prior versions of the SOFTWARE PRODUCT. However, if the SOFTWARE PRODUCT is marked "Not for Resale" or "NFR", you may not resell it or otherwise transfer it for value.

2.6   Copyright. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, programs and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by POLYCOM or its suppliers. Title, ownership rights, and intellectual property rights in the SOFTWARE PRODUCT shall remain in POLYCOM or its suppliers. Title and related rights in the content accessed through the SOFTWARE PRODUCT is the property of such content owner and may be protected by applicable law. This Agreement gives you no rights in such content.

2.7   Confidentiality. The SOFTWARE PRODUCT contains valuable proprietary information and trade secrets of POLYCOM and its suppliers that remains the property of POLYCOM. You shall protect the confidentiality of, and avoid disclosure and unauthorized use of, the SOFTWARE PRODUCT.

2.8   Dual-Media Software. You may receive the SOFTWARE PRODUCT in more than one medium. Regardless of the type or size of medium you receive, you may use only one medium that is appropriate for your single PRODUCT. You may not use or install the other medium on another PRODUCT.

2.9   Reservation of Rights. POLYCOM and its suppliers reserve all rights in the SOFTWARE PRODUCT not expressly granted to you in this Agreement.

2.10   Additional Obligations. You are responsible for all equipment and any third party fees (such as carrier charges, internet fees, or provider or airtime charges) necessary to access the SOFTWARE PRODUCT.

2.11 Additional Software. You may not install, access, or use any software on the PRODUCT unless such software was provided by or otherwise authorized by POLYCOM. POLYCOM may, in its sole discretion and in accordance with this Agreement or other applicable licenses, allow you to download and install certain support software on the PRODUCT, such as anti-virus software.

2.12 Benchmark Tests. You may not publish the results of any benchmark tests run on the PRODUCT, SOFTWARE PRODUCT, or any component of the SOFTWARE PRODUCT without written permission from Polycom.

3.   SUPPORT SERVICES. POLYCOM may provide you with support services related to the SOFTWARE PRODUCT ("SUPPORT SERVICES "). Use of SUPPORT SERVICES is governed by the POLYCOM policies and programs described in the POLYCOM-provided materials. Any supplemental software code provided to you as part of the SUPPORT SERVICES is considered part of the SOFTWARE PRODUCT and is subject to the terms and conditions of this Agreement. With respect to technical information you provide to POLYCOM as part of the SUPPORT SERVICES, POLYCOM may use such information for its business purposes, including for product support and development. POLYCOM will not utilize such technical information in a form that personally identifies you.

4.   TERMINATION. This Agreement will terminate automatically if you fail to comply with any of the terms and conditions of this Agreement. Polycom shall have the right to audit your use of the SOFTWARE PRODUCT in conjunction with this Agreement, and you will provide reasonable assistance for this purpose. In the event of any termination, you must cease use of the SOFTWARE PRODUCT, and destroy all copies of the SOFTWARE PRODUCT and all of its component parts. You may terminate this Agreement at any time by destroying the SOFTWARE PRODUCT and all of its component parts. Termination of this Agreement shall not prevent POLYCOM or its suppliers from claiming any further damages. If you do not comply with any of the above restrictions, this license will terminate and you will be liable to POLYCOM and its suppliers for damages or losses caused by your non-compliance. The waiver by POLYCOM of a specific breach or default shall not constitute the waiver of any subsequent breach or default.

5.   UPGRADES. If the SOFTWARE PRODUCT is labeled as an upgrade or update, you must be properly licensed to use the software identified by POLYCOM as being eligible for the upgrade or update in order to use the SOFTWARE PRODUCT.   A SOFTWARE PRODUCT labeled as an upgrade or update replaces and/or

supplements the software that formed the basis for your eligibility for the upgrade or update. You may use the resulting upgraded/updated SOFTWARE PRODUCT only in accordance with the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade or update of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single SOFTWARE PRODUCT package and may not be separated for use on more than one PRODUCT. You shall maintain the SOFTWARE PRODUCT replaced by the upgrade or update solely for use as an archival copy for recovery purposes for the updated PRODUCT.

6.   WARRANTY AND WARRANTY EXCLUSIONS.

6.1   Limited Warranty. Except as otherwise set forth in a Third Party License or in third party license terms set forth below, POLYCOM warrants that (a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of shipment by POLYCOM, and (b) any SUPPORT SERVICES provided by POLYCOM shall be substantially as described in applicable written materials provided to you by POLYCOM. POLYCOM DOES NOT WARRANT THAT YOUR USE OF THE SOFTWARE PRODUCT WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT ALL DEFECTS IN THE SOFTWARE PRODUCT WILL BE CORRECTED. YOU ASSUME FULL RESPONSIBILITY FOR THE SELECTION OF THE SOFTWARE PRODUCT TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM THE SOFTWARE PRODUCT. POLYCOM'S SOLE OBLIGATION UNDER THIS EXPRESS WARRANTY SHALL BE, AT POLYCOM'S OPTION AND EXPENSE, TO REFUND THE PURCHASE PRICE PAID BY YOU FOR ANY DEFECTIVE SOFTWARE PRODUCT WHICH IS RETURNED TO POLYCOM WITH A COPY OF YOUR RECEIPT, OR TO REPLACE ANY DEFECTIVE MEDIA WITH SOFTWARE WHICH SUBSTANTIALLY CONFORMS TO APPLICABLE POLYCOM PUBLISHED SPECIFICATIONS. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30 days, whichever is longer.

6.2   Warranties Exclusive. IF THE SOFTWARE PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, YOUR SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT POLYCOM'S SOLE OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. POLYCOM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF THE SOFTWARE PRODUCT. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM POLYCOM OR THROUGH OR FROM THE SOFTWARE PRODUCT SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT.

NEITHER POLYCOM NOR ITS SUPPLIERS SHALL BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE SOFTWARE PRODUCT DOES NOT EXIST OR WAS CAUSED BY YOUR OR ANY THIRD PARTY'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

7.   LIMITATION OF LIABILITY. YOUR USE OF THE SOFTWARE PRODUCT IS AT YOUR SOLE RISK. YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF THE SOFTWARE PRODUCT. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION DAMAGES FOR LOSS OF BUSINESS PROFITS OR REVENUE; BUSINESS INTERRUPTION OR WORK STOPPAGE; COMPUTER FAILURE OR MALFUNCTION; LOSS OF BUSINESS INFORMATION, DATA OR DATA USE; LOSS OF GOODWILL; OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF POLYCOM OR ITS SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, I NO EVENT SHALL POLYCOM'S SUPPLIERS BE LIABLE FOR ANY DIRECT DAMAGES WHATSOEVER ARISING OUT OF THE USE OR THE INABILITY TO USE THE SOFTWARE PRODUCT. IN ANY CASE, POLYCOM'S ENTIRE LIABILITY SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR U.S. $5.00. PROVIDED, HOWEVER, IF YOU HAVE ENTERED INTO

A POLYCOM SUPPORT SERVICES AGREEMENT, POLYCOM'S ENTIRE LIABILITY REGARDING SUPPORT SERVICES SHALL BE GOVERNED BY THE TERMS OF THAT AGREEMENT.

8.   INDEMNITY. You agree to indemnify and hold harmless POLYCOM and its subsidiaries, affiliates, officers, agents, co-branders, customers, suppliers or other partners, and employees, from any loss, claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your use of the SOFTWARE PRODUCT, your connection to the SOFTWARE PRODUCT, or your violation of the Terms.

9.   DISCLAIMER. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for death or personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety due to local law, they will be limited to the duration of the applicable warranty.

10.   EXPORT CONTROLS. You acknowledge that the SOFTWARE PRODUCT may be subject to export restrictions of various countries. You shall fully comply with all applicable export license restrictions and requirements as well as with all laws and regulations relating to the importation of the SOFTWARE PRODUCT, in the United States and in any foreign jurisdiction in which the SOFTWARE PRODUCT is used. Without limiting the foregoing, the SOFTWARE PRODUCT may not be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) any country to which the U.S. has embargoed goods; (ii) any end user known, or having reason to be known, will utilize them in the design, development or production of nuclear, chemical or biological weapons; or (iii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using the SOFTWARE PRODUCT, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. If you obtained this SOFTWARE PRODUCT outside of the United States, you are also agreeing that you will not export or re-export it in violation of the laws of the country in which it was obtained. You further acknowledge that the SOFTWARE PRODUCT may include technical data subject to export and re-export restrictions imposed by US law.

11.   MISCELLANEOUS.

11.1   Governing Law. This Agreement shall be governed by the laws of the state of California as such laws are applied to agreements entered into and to be performed entirely within California between California residents, and by the laws of the United States, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods (1980) and the Uniform Computer Information Transactions Act (UCITA) are hereby excluded in their entirety from application to this Agreement.

11.2   Entire Agreement. This Agreement represents the complete agreement concerning the SOFTWARE PRODUCT and may be amended only by a writing executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

11.3   Contact. If you have any questions concerning this Agreement, or if you desire to contact POLYCOM for any reason, please contact the POLYCOM office serving your country.

11.4   U.S. Government Restricted Rights. The software and documentation provided by Polycom pursuant to this Agreement are "Commercial Items," as the term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are licensed to United States Government end users (1) only as Commercial Items and (2) with only those rights as are granted to all other users pursuant to the terms of this Agreement.

11.5 High Risk Activities. The SOFTWARE PRODUCT is not fault-tolerant and is not designed or Intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the SOFTWARE PRODUCT could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). POLYCOM AND ITS

SUPPLIERS EXPRESSLY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

12.   THIRD PARTY SOFTWARE. The SOFTWARE PRODUCT may be distributed with software governed by licenses from third parties ("Third Party Software" and "Third Party License"). Any Third Party Software is licensed to you subject to the terms and conditions of the corresponding Third Party License, notwithstanding anything to the contrary in this Agreement. More information on Third Party Licenses included in the SOFTWARE PRODUCT can be found in the documentation for each PRODUCT. Polycom makes no representation or warranty concerning Third Party Software and shall have no obligation or liability with respect to Third Party Software. If the Third Party Licenses include licenses that provide for the availability of source code and the corresponding source code is not included with the Software, then check the documentation supplied with each PRODUCT to learn how to obtain such source code.

BY INSTALLING, COPYING, OR OTHERWISE USING THIS SOFTWARE PRODUCT YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS INDICATED ABOVE.

Polycom, Inc. © 2010. ALL RIGHTS RESERVED.
4750 Willow Road
Pleasanton, CA 94588
U.S.A.

***

McAFEE, INC. LICENSE TERMS ("McAfee")

For McAfee AV SDK ("McAfee Software")

In addition to the license terms above for the SOFTWARE PRODUCT, the following terms apply solely to McAfee Software:

1. "McAfee" means (a) McAfee, Inc., a Delaware corporation, with offices located at 3965 Freedom Circle, Santa Clara, California 95054, USA if the McAfee Software is purchased in the United States, Mexico, Central America, South America, or the Caribbean; (b) McAfee Ireland Limited, with offices located at 11 Eastgate Business Park, Little Island, Cork, Ireland if the McAfee Software is purchased in Canada, Europe, the Middle East, Africa, Asia, or the Pacific Rim; and (c) McAfee Co., Ltd. with offices located at Shibuya Mark City West Building 12-1, Dogenzaka 1-Chrome, Shibuya-ku, Tokyo 150-0043, Japan if the Software is purchased in Japan.

2. Limited Warranty. McAfee warrants that for sixty (60) days from the date of original purchase of the SOFTWARE PRODUCT, McAfee Software will be free from defects in materials and workmanship.

3. Remedies. McAfee's and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee's option, either (i) return of the purchase price you paid for the license, or (ii) replacement of the defective media in which the McAfee Software is contained. You must return the defective media to McAfee at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent McAfee is subject to restrictions under United States export control laws and regulations.

4. Warranty Disclaimer. Except for the limited warranty set forth herein, THE MCAFEE SOFTWARE IS PROVIDED "AS IS" AND MCAFEE MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW. MCAFEE, ITS SUPPLIERS AND AUTHORIZED PATNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR

OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR FITNESS FOR A PARTICULAR PURPOSE. YOU ASSUME RESPONSIBILITY FOR SELECTING THE MCAFEE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE MCAFEE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, MCAFEE MAKES NO WARRANTY THAT THE MCAFEE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE MCAFEE SOFTWARE WILL MEET YOUR REQUIREMENTS.

5. Notice to United States Government End Users. The McAfee Software and its accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

6. Governing Law. Any claims related to the McAfee Software will be governed by and construed in accordance with the substantive laws in force: (a) in the State of New York, if you purchased the McAfee Software in the United States, Mexico, Central America, South America, or the Caribbean; (b) in the Republic of Ireland, if you purchased the McAfee Software in Canada, Europe, Middle East, Africa, Asia, or the region commonly referred to as the Pacific Rim; and (c) in Japan if you purchased the McAfee Software in Japan. If you purchased the Software in any other country, then the substantive laws of the Republic of Ireland shall apply, unless another local law is required to be applied. This Agreement will not be governed by the conflict of laws rules of any jurisdiction or the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. The United States District Court for the Southern District of New York, and the Courts of New York County, New York, when New York law applies, the courts of the Republic of Ireland, when the law of Ireland applies, and the courts of Japan when Japanese law applies, shall each have non-exclusive jurisdiction over all disputes relating to the McAfee Software.

7. Free Software. The McAfee Software includes or may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL, which is distributed to someone in an executable binary format that the source code also be made available to those users. For any such software, the source code is made available in a designated directory created by installation of the McAfee Software or designated internet page. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.

8. Privacy. By utilizing the McAfee Software, you agree that the McAfee privacy policy, as it exists at any relevant time, shall be applicable to you. The most current privacy policy can be found on the McAfee web site (www.McAfee.com). By entering into this Agreement, you agree to the transfer of your personal information to McAfee's offices in the United States and other countries outside of your own.

9. Collection of Certain System Information. McAfee employs certain applications and tools through its website and within the McAfee Software, to retrieve information about your computer system to assist us in the provision and support of McAfee Software that you have chosen to subscribe to or use. This information is essential to enable us to provide you with quality service and up to the minute threat protection; and for these reasons, there is no opt-out available for this information collection.

10. Audit. McAfee may, at its expense and upon reasonable notice to you, perform an audit of your compliance with the terms of this Agreement. You understand and acknowledge that McAfee utilizes a

number of methods to verify and support the McAfee Software licensed for use by its customers. These methods may include technological features to prevent unauthorized use of the McAfee Software and to automatically report information about -- and verification of -- your deployment of McAfee Software. The information reported back to McAfee can also include: other McAfee products; other Software installed with or used by components of the McAfee Software; and third-party Software installed separately by customer but are integrated for use with McAfee Software In the event that McAfee requests a report for confirmation, you agree to provide a system generated report verifying your software deployment within thirty (30) days, such request to occur no more than four (4) times per year. In the event that McAfee requires a physical audit, such audit shall be preceded by thirty (30) days written notice and shall occur no more than once per year unless otherwise required for compliance with the Sarbanes-Oxley Act.

11. Auto-Boot /Post Boot Mode. McAfee shall have no liability to you for any damages resulting from the use of the McAfee Software in the "auto-boot" or "post-boot" mode. You are advised that such tools are designed for product deployment purposes only, and any other use does not provide adequate data security. Any such contrary use shall be at your sole risk. Moreover, in the event of a data breach resulting from such contrary use, you shall not publicize McAfee's name in connection with such breach, nor make any statements that unfairly disparage the reputation of McAfee products.

12. McAfee Customer Contact. If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call (408) 992-8599 or (866) 622-3911, FAX to (972) 963-7001, or write: McAfee, Inc., Attention: Customer Service, 5000 Headquarters Drive, Plano, TX 75024, or e-mail to http://www.mcafeehelp.com. Alternatively, you may contact your local McAfee entity at the number listed at http://www.McAfee.com.

Corrections and Known Limitations

Corrections

Corrections Between Version 5.1.0.G and Version 7.5.0.J

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J*

#	Category	Key	Description	Detected in Version	Workaround
1	*Audio*	VNGR-16038	On an RMX with two MPMx cards, when connecting two dial-out PSTN participants, there is no audio between them.	V7.0	
2	*Calendaring*	VNGR-13703	No Active Alarm or error message when defining incorrect parameters of the Exchange server on the RMX.	V6.0	
3	*Cascading*	VNGR-15023	Content cannot be sent via cascade link. Video Disconnection Cause of the link participant is displayed as: "Content media was not established because the remote endpoint does not support the conference content protocol."	V6.0	
4	*CDR*	VNGR-11586	Wrong GMT Offset in RMX CDR file. It does not include the minutes.	V4.0.1	
5	*CDR*	VNGR-11691	Wrong GMT Offset in RMX CDR file. It does not include the minutes.	V4.0.1	
6	*Content*	VNGR-16661	On an RMX 1500 running an 1024Kbps HD720p conference with Video Clarity, Auto Terminate, Sharpness, Encryption, LPR, Echo Suppression and Auto Layout enabled, when sending content some dial-out HDX9004 endpoints had bad video.	V7.0	

Table 6 *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
7	*Content*	VNGR-16732	When sending content, the line rate of the sender endpoint decreases and when content is stopped, the line rate increases, above the conference line rate. For example, if the conference line rate is set to 512Kbps, it decreases to 300Kbps when sending content and it increases to 700Kbps when the content is stopped.	V7.0	
8	*Content*	VNGR-16502	In a 1920Kbps conference with H.264 content, after HDXs view and receive content, then when an VSX3000 endpoint connects the content halts and an error message appears: "0x80c7a4cCMfaTask::On BadSpontIndFromMFA reason: 1, description: Decoder resource allocation error! Closing decoder port! "	V7.0	
9	*Content*	VNGR-17027	Black screen or frozen content displayed when endpoints dial into the conference via DMA.	V7.0	
10	*Content*	VNGR-16734	On an RMX 1500 running an 768Kbps conference with LPR, Gathering, Sharpness, Auto Layout, Echo Suppression, Audio Clarity and Send Content to Legacy Endpoints enabled, when sending content from the Sony XG80 endpoint, HDX7600 endpoints do not view content.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
11	*Content*	VNGR-12225	In a conference running at a line rate of 768 Kbps with HDX endpoints connected and Content that is set to Graphics is sent or VSX endpoint connects the line rate decrease to 512 Kbps and does not increase back to 768 Kbps when Content is halted or the VSX endpoint disconnects.	V5.0.0	
12	*Content*	VNGR-12342	When adding two or more Legacy endpoints to an ongoing conference, ViewStation endpoints do not revert back to Conference Layout after content sharing is halted.	V4.1	
13	*Content*	VNGR-13465	An assert occurs when sending Content from a VSX 3000 endpoint to a conference that includes a recording link and MOC (SIP URI), HDX SIP, VSX 3000 H323 are connecting to it.	V6.0	
14	*Content*	VNGR-14791	Artifacts can be seen around the layout lines and site names when endpoints (HDX 8000,HDX 9004,HDX 4000.CMAD,PSTN) connect to a conference running on an RMX in MPM mode, at a line rate of 512 Kbps and Content is sent to all endpoints.	V6.0	
15	*Diagnostics*	VNGR-16893	On an RMX2000 with MPM cards, when implementing the Diagnostic mode the MPM card status remains in a "startup" phase.	V7.0	
16	*Diagnostics*	VNGR-16633	On an RMX 2000/4000 when accessing the Diagnostic mode and clicking the "run all tests" option, the confirmation window only appears minimized in the Windows Toolbar at the bottom of the screen.	V7.0	

Table 6 *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
17	*Encryption*	VNGR-12212	FX ISDN endpoints cannot connect to encrypted conferences.	V5.0.0	
18	*Gateway*	VNGR-16533	Intermittent blurred video or green blocks displayed on HDX H.320 call connected via 1024kbps Gateway call via RMX 2000 with MPMx.	V7.0	
19	*Gateway*	VNGR-16603	When the endpoint that initiates a Gateway call disconnects, the Gateway session is not terminated while others are still in the conference. The Gateway session should terminate.	V7.0	
20	*Gateway*	VNGR-12018	When an endpoint connects through MGC Gateway, the layout is automatically defined as 1x1 'Personal' layout instead of applying the conference layout.	V5.0.0	
21	*General*	VNGR-15745	When you try to add the flag: "REDIAL_INTERVAL_IN_ SECONDS" in the System Configuration an error code appears: 30432.	V7.0	
22	*General*	VNGR-16457	Critical fan alert is displayed in the RMX Hardware Monitor in Event Log properties box while in the Hardware Monitor pane the system status is displayed correctly as Normal.	V7.0	
23	*General*	VNGR-17454	An MCU internal problem occurred: "ConfPartyMcuInternalProblem - Party:2467 Conf:744 receives Failure Status for opcode: CONFPARTY_CM_OPEN _UDP_PORT_REQ Req:799954. "	V7.0.1	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
24	*General*	VNGR-16931	RMX 2000 with MPM+ displays empty video window in layout in ISDN + IP mixed conference during load test.	V7.0	
25	*General*	VNGR-16691	In ICE environment, when a local endpoint connects to the conference, the connection type in the Participant Properties should be Local instead of Host.	V7.0	
26	*General*	VNGR-11703	Sometimes participants do not connect when the RMX is running under load. The disconnection cause is stated as "MCU internal problem 32121".	V4.5	
27	*General*	VNGR-14276	When the MCU is in start up mode, the upgrade status bar does not appear.	V6.0	
28	*General*	VNGR-15374	On an RMX with MPMx cards, when a number of endpoints with different line rates dial-out, some endpoints do not connect.	V7.0	
29	*General*	VNGR-15506	In the RMX Web Client, login as Administrator and create a new user "KANSA" with Auditor permissions. Logout and login using the new Auditor user, an error message appears.	V7.0	
30	*General*	VNGR-15629	When you start a conference from an existing conference template, a popup message appears: "The conference ID already in use". Conference does not start.	V7.0	
31	*General*	VNGR-15648	In a conference started from the default "Factory_Video_Profile" and with "Send Contents to Legacy Endpoint" enabled, Legacy & ViewStation Endpoints cannot view content.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
32	*General*	VNGR-15723	When a conference is created with the same name as another conference already running, an incorrect error message appears: "Failed to add conference: 2501".	V7.0	
33	*General*	VNGR-15726	The "Display repetition" option should be disabled when in Static Mode.	V7.0	
34	*General*	VNGR-15728	When Auto Layout is enabled in a conference, the Auto Layout function does not select the appropriate layout for number of participants present in the conference.	V7.0	
35	*General*	VNGR-15740	After updating the Exchange Integration Configuration window and clicking OK, a Message alert "31006" does not provide you with any information as to the cause of the error.	V7.0	
36	*General*	VNGR-15741	When modifying the Port Gauge usage percentage from the default value ("80%") to a lower value ("40%" or "60%"), an error message is displayed. The error message is not translated into the UI language.	V7.0	
37	*General*	VNGR-15743	In the Ping Dialog box, when clicking Ping an error message appears instead of receiving an IP address.	V7.0	
38	*General*	VNGR-15744	In the Ping Dialog box, when clicking Ping an error message appears instead of receiving an IP address.	V7.0	
39	*General*	VNGR-15808	After modifying settings in the IP Network Services, the "Reset MCU" message did not appear, nor was the IP Network Service updated.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
40	*General*	VNGR-15932	In the Web Client set to Japanese, when selecting Software download, click "Browse" you cannot view the binary download file.	V7.0	
41	*General*	VNGR-15933	When accessing the English version of the RMX Web Client, when viewing properties of the conference profile, some of the fields are in Japanese.	V7.0	
42	*General*	VNGR-15934	In the RMX Web Client, when creating a new gateway profile and clicking OK, a wrong message appears: "Conference name already exists". The message should be: "Failed to add Gateway Profile: Display name already exists".	V7.0	
43	*General*	VNGR-15949	After upgrading the RMX to version 7.0, RMX IP address is not displayed.	V7.0	
44	*General*	VNGR-15950	In the Management Network Properties - IP tab, when selecting ON [Secured Communication] and clicking OK, the popup message states RMS instead of RMX.	V7.0	
45	*General*	VNGR-15951	When Dialing in from a PSTN participant to an EQ when entering the DTMF the participant cannot connect.	V7.0	
46	*General*	VNGR-15952	When viewing the properties of the Entry Queue when selecting "IVR service provider only" and clicking [OK], when re-opening the Entry Queue properties, the "IVR service provider only" is not selected.	V7.0	

Table 6 *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
47	*General*	VNGR-16075	On an RMX 2000 with a 384Kbps conference started from a Profile with three endpoints connected, when the last endpoints disconnects an assert appears: 32112.	V7.0	
48	*General*	VNGR-16266	In RMX Web Client, when viewing the Restore Factory Defaults window the "Select the Backup & Continue button to save the current configuration and restore factory defaults" field is not translated properly in Japanese.	V7.0	
49	*General*	VNGR-16293	On an RMX 4000 with the MPM+ card, a "CureDump ConfParty" file is created and saved on file.	V7.0	
50	*General*	VNGR-16348	On an RMX with the MPM card and version 7.0, when a conference is started from a Template with ViewStation 512/EX endpoints, the system restarts unexpectedly.	V7.0	
51	*General*	VNGR-16397	On the RMX 1500, in the IP Network Service > Management Network > the Lan Ports tab appears. It should be the IP tab.	V7.0	
52	*General*	VNGR-16400	When a conference is active on the RMX 1500, in the Hardware Monitor - LAN Properties there is an "Status" indication that the LAN Media is "Inactive". It should state "active".	V7.0	
53	*General*	VNGR-16421	When a HDX (A) endpoint dials the following string: "Prefix_ID of the Gateway Profile *ISDN", to the number of the second HDX using an IP to ISDN call and starts a 384Kbps conference with IVR enabled, if HDX A sends content to HDX B, the HDX views a black screen.	V7.0	Connect both HDXs directly to a regular conference that is using the same profile as the GW profile.

POLYCOM®

Table 6 *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
54	*General*	VNGR-10100	When the RMX is set to Flexible Allocation Mode and more than 14 endpoints are connected to a single MPM+80 card in line rates above 2Mbps, video artifacts may appear.	V4.0.1	Change the resource Allocation Mode to Fixed Mode.
55	*General*	VNGR-10341	When the "$" sign is included in the User password logged into RMX Ver 3.0 or 4.0, access to Hardware Monitor is denied and an error message is displayed.	V4.0.0	
56	*General*	VNGR-10366	After deleting an ISDN/PSTN Network Service, text that appears in the message alert is inconsistent.	V4.1	
57	*General*	VNGR-10884	When the Resource Capacity Mode is set to Flexible and the Port Configuration slider is moved, an incorrect message displays, requesting that the RMX be reset.	V4.1	Ignore the message.
58	*General*	VNGR-11970	A Power OFF error message appears on the MPM+ cards on an RMX that has been running 20 conferences at a line rate of 1472 Kbps with four HD720p dial-in participants in each conference when terminating all the conferences after 90 minutes and restarting them immediately.	V5.0.0	
59	*General*	VNGR-12241	Sometimes, after 8 hours or more of conferencing at line rates of 4Mbps in a highly loaded MCU, the video processing unit fails.	V5.0.0	
60	*Hardware*	VNGR-16898	On an RMX 4000 with MPMx_D cards in the Diagnostic mode, when running card monitoring tests on the RTM_ISDN card the tests fail.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
61	*Hardware*	VNGR-16882	On an RMX 1500 in the Diagnostic mode, when viewing the MCU Monitor section, the card slot numbering is incorrect.	V7.0	
62	*Hardware*	VNGR-16166	On an RMX 2000 with two MPM+ cards, after several minutes participants could not connect due to MCU Internal Problem 32112.	V7.0	
63	*Hardware*	VNGR-15801	After upgrading RMX4000, an error message appears: "No RTM-LAN or RTM-ISDN installed" on slots13, 14, 15". In fact no RTM-ISDN card is installed in slot 13.	V7.0	
64	*Hardware*	VNGR-12059	After upgrading to build version 5.0.0.21, the temperature on the card reached Major and required attention.	V5.0.0	
65	*Interoperability*	VNGR-16647	On an RMX 2000 in a 384Kbps H.323 CP conference with Sharpness and LPR enabled, when the RMX dials-out to an Tandberg 6000E, an empty video frame appears.	V7.0	
66	*Interoperability*	VNGR-16723	On an RMX 1500 running an mixed (H.323, SIP & ISDN) 1024Kbps conference, after connecting the ISDN endpoint and changing the layout, after a few minutes the ISDN endpoint views a black screen and the video frame rate is 0.	V7.0	
67	*Interoperability*	VNGR-16829	Blurred and highly color saturated video, followed by a black screen is displayed on HDX ISDN endpoint connected to RMX 2000 with MPMx at 1152kbps.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
68	*Interoperability*	VNGR-16902	RMX with MPMx connected via H.320 to Tandberg 6000 B endpoint is listed with "Connected With Problem" status.	V7.0	
69	*Interoperability*	VNGR-17384	Loss of lip sync occurs on HDX8000 endpoint that dialed via DMA with higher line rate than the conference (512) to RMX2000 running V7.0.1.16 with 2*MPM+80 cards.		
70	*Interoperability*	VNGR-16707	An RMX 2000 running an 1920Kbps CP conference with LPR, Gathering and Sharpness enabled, when the RMX dials-out to an H.323 HDX endpoint, the HDX displays blue patchy video.	V7.0	
71	*Interoperability*	VNGR-16616	CMAD negotiates G.711u instead of G.719 when connecting to a conference running at a line rate of 64Kbps, video quality is set to sharpness, and auto layout is enabled.	V7.0	
72	*Interoperability*	VNGR-16959	On RMX running H.323, 384kbps conference with MPM+ or MPMx with Send Content to Legacy Endpoints enabled. When HDX9004 sends content iPower9000 endpoint receives content while FX endpoint does not.	V7.0	
73	*Interoperability*	VNGR-15936	When using Japanese characters in the display name of VVX1500-175/ VVX1500-176 endpoints, the endpoints display only a number.	V7.0	
74	*Interoperability*	VNGR-16398	In a 1920Kbps conference with LPR enabled, when connecting 3 HDX endpoints bad video appears.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
75	*Interoperability*	VNGR-10880	VSX6000/VSX3000 endpoints receive incorrect protocol and format in a encrypted conference with LPR enabled.	V4.0.1	
76	*Interoperability*	VNGR-11412	In a CP Conference with the Video Quality set to Sharpness, VSX6000 and V500 H.323 endpoints encounter video stills.	V4.1	
77	*Interoperability*	VNGR-11508	When endpoints connect to a conference running on the RMX through the DMA, the endpoints will see full screen (1x1) layout and not the conference layout.	V4.1	
78	*Interoperability*	VNGR-11753	Picture is horizontally stretched on the ISDN endpoint behind Codian ISDN Gateway, despite changing video display settings on the endpoint.	V4.1	
79	*Interoperability*	VNGR-11854	When Ipower v6.2.0.1208 connects to RMX V.4.1 with Siren 14 or G722.1, the audio is garbled / chopped.	V4.0.1	
80	*Interoperability*	VNGR-11881	Garbled audio is heard or audio is muted altogether when dialing from PVX to other endpoints via RMX version 4.1.	V4.1	
81	*Interoperability*	VNGR-11882	A PVX endpoint sometimes cannot receive H.239 content from an RMX 2000.	V5.0.0	
82	*Interoperability*	VNGR-11959	When the RMX is used as a gateway to route audio calls to the DMA that run conferences on RMX with a version earlier than 4.1.1, the audio endpoints fail to connect to these conferences.	V4.1.1	Use RMX version 4.1.1 or later.
83	*Interoperability*	VNGR-11962	A loud buzzing noise occurs when a Tandberg MXP endpoint connects to a conference using ISDN with AES encryption set to Auto.	V5.0.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
84	*Interoperability*	VNGR-12069	In a conference running at a line rate of 1920Kpbs, with LPR and AES enabled, H.320 Tandberg MXP dial-in participants cannot connect and an assert appears.	V5.0.0	
85	*Interoperability*	VNGR-9928	When sending content from CMAD in a 384Kbps call, changes in the video image are observed.	V3.0.0	
86	*IP*	VNGR-12255	Occasionally, problems are encountered with the Gatekeeper and memory. The process recovers seamlessly without effecting the overall experience.	V5.0.0	
87	*ISDN*	VNGR-16642	On RMX 1500 running a conference started from a conference profile, when a Viewstation MP512 ISDN endpoint connects, an error message appears: "Connected With Problem".	V7.0	
88	*ISDN*	VNGR-16855	Video freezes on ISDN endpoints in a fully loaded RMX 1500 when connecting, disconnecting and reconnecting all the endpoints.	V7.0	
89	*ISDN*	VNGR-11392	No Voice Activated Switching when an ISDN Video participant is connected to a conference running on RMX version 4.0.	V4.0.0	
90	*ISDN*	VNGR-11672	Sony PCS-1600s endpoint cannot connect using ISDN lines.	V4.1	Set the flag ISDN_LEGACY_EP_CLOSE_CONTENT_FORCE_H263 to Yes

Table 6 *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
91	*IVR*	VNGR-15663	An IVR slide with1080p resolution was uploaded successfully to the RMX but cannot be viewed with the preview button nor could be seen in the IVR welcome slide.	V7.0	
92	*IVR*	VNGR-10824	In a SIP CP conference with a line rate of 2 Mb, HDX 8006 endpoints cannot view the IVR slide.	V4.1	
93	*IVR*	VNGR-11773	On rare occasions, the IVR audio message may be played at a higher speed than normal.	V4.1.1	
94	*IVR*	VNGR-12021	A conference running at a line rate of 1920Kbpsand IVR Service that includes a Welcome Slide, both the Welcome Slide and Video are partially blacked out.	V5.0.0	
95	*IVR*	VNGR-9191	When DTMF codes have been entered by the participants, the volume of the IVR Message may be suppressed or the message may be cut.	V4.0.0	
96	*IVR-RMX 4000*	VNGR-16548	On the RMX 4000 & MPMx card, when running an 4MB CP conference, the Welcome slide does not appear.	V7.0	
97	*IVR-RMX 4000*	VNGR-12283	On the RMX 4000, when dialing from ISDN endpoint to GW, the IVR Welcome message is cut off.	V5.0.0	
98	*IVR-RMX 4000*	VNGR-12508	When an endpoint connects to a Meeting Room on the RMX4000, the RMX2000 Welcome slide is displayed.	V5.0.0	
99	*IVR-RMX 4000*	VNGR-19175	On an RMX 4000 in the Ultra Secure Mode, when a dial-out conference is started from a Profile and the IVR initiates, audio and video problems occur.	7.5	

POLYCOM®

Table 6   Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)

#	Category	Key	Description	Detected in Version	Workaround
100	*LPR*	VNGR-11020	Reduced video quality may be observed when using LPR with HD720p. When packet loss is detected by the LPR mechanism, the LPR lowers the call bit rate to keep the video quality of the call. When excessive packet loss exists, the call rate may drop down to 128K, using HD 720p under these conditions will result in a reduced video image quality.	V4.1	
101	*Multilingual*	VNGR-16904	Incorrect Japanese translation of "Restore Last Version".	V7.0	
102	*Multilingual*	VNGR-12096	After selecting French or Japanese and logging out of the Web Client, when repeating the Log-in/out process the UI appears in English.	V5.0.0	
103	*Multilingual*	VNGR-12425	After creating a new gateway, using the Japanese RMX Web Client, the pop-up message has the wrong description.	V5.0.0	
104	*Multilingual*	VNGR-12426	In the Japanese RMX Web Client, the New Profile > Advanced tab several field names are not translated.	V5.0.0	
105	*Multilingual*	VNGR-12427	In the New Reservation dialog box, several translations are missing in Japanese.	V5.0.0	
106	*Multilingual*	VNGR-12453	After deleting a conference, a confirmations message appears in English instead of Japanese.	V5.0.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
107	*Partners - Microsoft*	VNGR-16833	When using RMX with MPM+ with ICE enabled in a Federation dialing configuration, the Microsoft Office Communicator Client is disconnected. Call Disconnection Cause is listed as "sip hw internal MCU problem - 0".	V7.0	
108	*Partners - Microsoft*	VNGR-16804	On RMX with MPMx, Microsoft Office Communicator Client connected at 384kbps doesn't recover and disconnects after Packet Loss after dial-in MOC Client changes LAN configuration to 100 Half Duplex during ongoing conference.	V7.0	
109	*PCM*	VNGR-16913	On RMX 4000 with MPM+, PCM on certain H.323 endpoints does not respond to arrow keys.	V7.0	
110	*Recording*	VNGR-11664	Recording links on RMX 4.0 do not support AES encryption, although the RSS v4.0 and above have an AES encryption option.	V4.0.2	
111	*Reservations*	VNGR-11635	When the duration of an ongoing conference with an ISDN dial in number is set to one minute and auto-extend is enabled, the RMX may not detect a conflict in ISDN dial-in number when placing a reservation on the RMX with an identical ISDN number. In case of a dial-in number conflict, incoming calls are routed to the ongoing conference and not to the reserved meeting.	V4.1	
112	*RMX 1500 General*	VNGR-16848	On RMX 1500, Media port is listed in the Ethernet Settings dialog box but not in the LAN List pane of the Hardware Monitor.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
113	*RMX 1500 General*	VNGR-16866	On RMX 1500 Message Overlay is blurred on SIP and H.323 endpoints.	V7.0	
114	*RMX 1500 general*	VNGR-16957	On RMX 1500 with MPMx High System CPU Usage fault occurs.	V7.0	
115	*RMX 1500 General*	VNGR-16423	On RMX 1500, changing the port speed setting from Auto to 100F is ignored with Auto remaining selected after reset.	V7.0	
116	*RMX 1500 Video*	VNGR-16766	On RMX 1500 with MPMx, strobe effect appears in video during H.323 call to HDX endpoints at 1080p at 4Mbps.	V7.0	
117	*RMX 4000*	VNGR-17007	No content display and several endpoints disconnected from the conference when content is sent during a conference running on RMX 4000 at a line rate of 1920Kbps and Send Content to Legacy Endpoints option enabled. Faults list indicated that the link between FSM 4000 and the media card was lost.	V7.0	
118	*RMX 4000*	VNGR-12298	When viewing the RTM LAN properties of RMX 4000 in the Hardware Monitor, no data is displayed.	V5.0.0	
119	*RMX Manager*	VNGR-12195	On Vista Operating Systems, when accessing the RMX Web Client and clicking Install RMX Manager, no installation is implemented.	V5.0.0	
120	*RMX Manager*	VNGR-14452	When using RMX Manager V5.1 and V6.0 to manage several RMXs and swapping between RMXs, the Gatekeeper Prefix displayed on the main screen is not updated according to the selected RMX.	V5.0.1	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
121	*SIP*	VNGR-17732	In ICE environment, if QoS is enabled in the IP Network Service, the connection to the OCS is broken and the RMX cannot provision ICE and cannot see the connection to the edge server.	V7.0/7.0.1	
122	*SIP*	VNGR-12136	No video or low quality video is seen by a SIP HDX endpoint that connects to a conference set to 384 Kbps at much higher line rate, such as 4Mb.	V4.6	
123	*SIP*	VNGR-15954	After creating a new SIP Factory and then deleting it, you cannot create another new SIP factory. A message alert appears: "fail to add SIP factory."	V7.0	
124	*SIP*	VNGR-11971	When trying to connect SIP participants via an external API application, when the URI and IP address fields are switched (the IP address is left empty and the URI is set to the IP address), the endpoint will disconnect.	V5.0.0	Set the IP address correctly.
125	*SIP*	VNGR-12017	Occasionally, when a dial-in SIP participant accesses the Entry Queue, the participant connection fails even though the participant entered the correct conference ID.	V5.0.0	
126	*Software Version*	VNGR-16803	On RMX 1500 with MPMx High System CPU Usage fault occurs.	V7.0	
127	*Software Version*	VNGR-16818	On RMX 2000 with MPM, after upgrading the RMX restarted with "no utilizable unit for audio controller" requiring hard reset (switch off and then on).	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
128	*Software Version*	VNGR-16845	When using RMX with MPMx, MplApiSocket disconnects for 10 seconds resulting in disconnection of all participants.	V7.0	
129	*Software Version*	VNGR-16915	On RMX 1500, Encryption Key Server can cause the MCU to display High CPU Usage alert after restart.	V7.0	
130	*Upgrade Process*	VNGR-16565	After upgrading to the RMX1500 to Ver 7.0.0.123 the following error message appears: "CardsComponent Type:switch, Description: Temperature problem - Major".	V7.0	
131	*Upgrade process*	VNGR-16430	On RMX 2000, MPL failure occurs after upgrading Version 7.0.	V7.0	
132	*Upgrade Process*	VNGR-16884	On an RMX2000/4000 when upgrading to version 7.0 build 139, the MPMx card on Hardware Monitor appears normal, but the MPMx card blinking LEDs indicate the card is still "startup" mode.	V7.0	
133	*Upgrade Process*	VNGR-14844	The Faults List is empty when upgrading the RMX 2000 from V5.01 build 24 to v6.0 build 86.	V6.0	
134	*Upgrade Process*	VNGR-16828	When upgrading RMX4000 7.0.0.136 with MPM+ to Version 7.0.0.142 or 7.0.0.145, MPL Failure was indicated and the RTM-IP still shows "in upgrade" while the RMX exits the "startup" indication.	V7.0	
135	*Upgrade Process*	VNGR-12389	When upgrading the RMX2000 from V4.1 to V5.0.0.23 after the software was uploaded an error message "Version download failed" appears.	V5.0.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
136	*Upgrade Process*	VNGR-14404	Loss of Connection to the Management Network and H323 Signaling Ports occurs immediately after upgrading RMX 4000 to version 5.0.1.23.	V5.0.1	
137	*Video*	VNGR-15557	On the RMX 4000 with a VSW conference set to 1080p30, when the RMX dials out to 3 HDX and 2 LifeSize endpoints, the HDX endpoints remain stuck in their splash screen.	V7.0	
138	*Video*	VNGR-16382	During a video conference on the RMX2000 with an MPMx card, bitrate overflow occurs when there's a lot of motion in the video.	V7.0	
139	*Video*	VNGR-16684	On an RMX 2000 with MPM+ cards running a 1920 Kbps conference using the following settings LPR, Sharpness and Video Clarity, when connecting ISDN endpoints metallic background noises can be heard. Connect an H.323 endpoint, then ISDN endpoints view their own video.	V7.0	
140	*Video*	VNGR-16760	On an RMX1500, when connecting seven HDX8006 endpoints to a 4096 Kbps & HD 1080p conference with Video Clarity, Sharpness, Echo Suppression and Auto Layout enabled, stripes appeared in the endpoints video.	V7.0	
141	*Video*	VNGR-16789	Connecting three HDX8006, six HDX9004 and nine V500 endpoints to a 1024 Kbps, HD 1080p conference running on an RMX1500, with Video Clarity, Echo Suppression and Auto Layout enabled, poor video motion was observed.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
142	*Video*	VNGR-17086	Video is frozen after 2-3 seconds when using CMA-D with VBP 4350 on RMX 2000 running V7.0.0.162 with MPMx.	V7.0	
143	*Video*	VNGR-17195	Colored stripes and video freeze occurs in 512 kbps calls dialed via DMA to RMX4000 running V7.0.0.162 with MPM+ cards.	V7.0	
144	*Video*	VNGR-17426/ 17324/ 17319	Periodic momentary freezing of video sent from ISDN endpoint is observed on H.323 endpoint when connected to a CP conference running on RMX 2000 with MPMx at a line rate of 1920kbps and AES and LPR options enabled.	V7.0.1	
145	*Video*	VNGR-17472/ 17379	Striped video image of all other participants occurs on HDX8000 endpoint after dialing via DMA to RMX4000 running V7.0.1.16 with, 4*MPM+80 cards.	V7.0.1	
146	*Video*	VNGR-16930	When connecting 15 HDX8006 endpoints to a 1024Kbps & HD 720p conference with Video Clarity, Sharpness, Echo Suppression and Auto Layout enabled, running on an RMX1500, the endpoints had low frame rates, frozen video, packet loss and incorrect video resolutions.	V7.0	
147	*Video*	VNGR-16910	On RMX with MPMx, High-Profile endpoints (HDX 8006) display green flash in video window of layout. Attempts to send content result in "MFA error" followed by shaking video on HDX 9004 endpoints.	V7.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
148	*Video*	VNGR-16888	When starting a conference from the default profile with 20-30 endpoints connected on an RMX 4000 with MPMx cards, changing the conference layout causes video freezes and empty layout cells appear.	V7.0	
149	*Video*	VNGR-16811	On RMX 1500 MPMx - S, when the HDX8006 endpoint at 720p resolution using High-Profile at 512kbps connect to the conference the participant experiences welcome slide flash in video or endpoint freezes with welcome slide displayed.	V7.0	
150	*Video*	VNGR-16711	On an RMX 2000 with MPMx cards, when dialing in at 384Kbps using VSX endpoints to a Meeting Room, the video transfer rate was 800Kbps instead of 384Kbps.	V7.0	
151	*Video*	VNGR-15543	On an RMX 4000 with a CP conference with Auto Layout and Sharpness enabled, Sony PCS-1 endpoints do not transmit video in H.320 calls.	V7.0	
152	*Video*	VNGR-14673	In a 4MB Immersive Telepresence conference with Sharpness enabled, cracking and popping sounds are heard.	V6.0	
153	*Video*	VNGR-14837	Gathering slide info is cut off for dial-out VSX and CMAD MAC endpoints that receive video at a resolution of 480x352. The gathering screen displays correctly on the HDX endpoints	V6.0	

Table 6   *Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)*

#	Category	Key	Description	Detected in Version	Workaround
154	*Video*	VNGR-15626	During a video conference audible clicks & popping sounds are heard during when the following endpoints are connected: CMAD, VSX3000, HDX6000 and HDX7000.	V7.0	
155	*Video*	VNGR-15717	In a 1MB conference with 2 HDX endpoints one with High Profile and the other without High Profile, corrupted video is viewed in the High Profile HDX endpoint.	V7.0	
156	*Video*	VNGR-15727	A 1024Kbps conference with maximum resolution forced to H720p, when connecting HDX endpoint with a resolution set to CIF, the endpoint connects with 4CIF thereby using more resources.	V7.0	
157	*Video*	VNGR-16289	On the RMX2000 running a conference based on the default Profile, when the RMX dials-out in SIP to the LifeSize endpoint, the call connects but the LifeSize endpoint does not view video.	V7.0	
158	*Video*	VNGR-16743	On an RMX 1500 running a 2048Kbps conference with LPR, Gathering, Sharpness, Send Content to Legacy Endpoints, Auto Layout, Echo Suppression and Audio Clarity enabled, when connecting all the endpoints together, after the gathering slide closes all HDX endpoints display low quality video.	V7.0	
159	*Video*	VNGR-16917	On an RMX2000 with MPMX cards, when connecting HDX8000 endpoints with 720p and 1080p resolutions using a 1+7 layout, green artifacts and stripes appear in the video.	V7.0	

Table 6 Corrections Between Version 5.1.0.G and Version 7.5.0.J (Continued)

#	Category	Key	Description	Detected in Version	Workaround
160	*Video*	VNGR-11257	When connecting a VSX3000 endpoint to a CP conference at a line rate of 4M and video quality set to Sharpness, video quality of the connected participants is affected.	V4.1	
161	*Video*	VNGR-11541	When the VVX1500 is forced to H.263 in SIP calls, the endpoint cannot receive video from the RMX.	V4.1	Do not force the VVX1500 to H.263.
162	*Video*	VNGR-11609	Incorrect video aspect ratio in full screen in mixed resolution conference running at a line rate of 384 Kbps and to which	4.1	
163	*Video*	VNGR-11680	Site names disappear from layout 4x4 or 1+10.	V4.1	
164	*Video*	VNGR-11697	Several HDX endpoints connected to a conference running on RMX version 4.1 at 1Mb at a lower resolution (4SIF instead of 720p).	V4.1	Disconnect and connect the endpoint.
165	*Video*	VNGR-12217	In a conference running at line rate of 4Mb and resolution of HD1080p, some HDX endpoints (H.323 & SIP) encounter video problems due to a DSP failure.	V5.0.0	
166	*Video*	VNGR-13311	When a VSX7000 IP endpoint joins a conference running at a line rate of 384 Kbps set to Sharpness with VSX6000, V500 and VSX7000 IP endpoints connected, the video resolution changes to 4CIF.	V4.1	

Corrections Between Version 4.5.0.F and Version 5.1.0.G

Table 7   *Corrections Between Version 4.5.0.F and Version 5.1.0G*

No	Category	Description	ID/ VNGR#
1	Cascade	Site names are displayed incorrectly when connecting endpoints to a cascaded conference that is already connected by the cascaded link.	12753 VNGFE-2278
2	Content	In a 768 Kbps conference with Content & H.264, HDX and VSX endpoints video rates were not increased after Content was terminated in the conference.	12225
3	Content	Legacy endpoints do not return to conference layout after Content is stopped.	12342/ 2283
4	Encryption	H.320 FX endpoint does not connect to the conference when encryption is turned on.	12212
5	Gateway	When an IP participant dials the Gateway Profile on RMX A and enter a destination conference ID of a conference running on RMX B, the participant connects correctly to the second RMX but the site name displays the name of RMX A instead of the endpoint name.	13334/12881 VNGFE-2377
6	General	RMX is showing "Overflow in /output" as the hard drive is not recognized by the controller.	13607/ VNGFE-2497
7	General	*Restore Factory Defaults* dialog box is translated incorrectly in Japanese.	12690/ VNGBE-810
8	General	When connecting to RMX 4000, default MCU *Display Name* is POLYCOM RMX 2000 instead of RMX 4000.	12689/ VNGBE-811
9	General	Sometimes, endpoints fail to connect to a conference after modifying the Profile assigned to that conference and a major alert "Power off" is displayed.	12618/ VNGBE-784
10	General	When logged in to RMX Web Client in Japanese and trying to download the software using A*dministration > Software Management > Software Download*, the *build.bin* file cannot be found.	12615/ VNGBE-782
11	General	When logged in to RMX Web Client in Japanese, the Telepresence value in Administration > System Information is displayed in English.	12518/ VNGBE-758
12	General	Incorrect Japanese translation of the error message displayed when creating an EQ and using a dial-in number already assigned to another conferencing entity.	12514/ VNGBE-773
13	General	In the Japanese RMX Web Client, the conference deletion message is displayed in English.	12453

Table 7   *Corrections Between Version 4.5.0.F and Version 5.1.0G (Continued)*

No	Category	Description	ID/ VNGR#
14	General	When logged in to RMX Web Client in Japanese and opening a file in the Auditor Viewer (Administration > Tools > Auditor Viewer, click local file icon), the dialog box title that is show in Japanese switches to English after opening the file.	12447/ VNGBE-755
15	General	In the Japanese RMX Web Client, the New Reservation > Schedule > Monthly option has an incorrect translation.	12427
16	General	Rarely, a false active alarm appears: "Temperature has reached a problematic level and requires attention" for no apparent reason.	12059
17	General	When an RTM LAN card is changed on an activated system, a Power off error message is displayed for all the MPM+ cards on the system, although the MCU continues to work normally.	11970
18	General	RMX status changes to Major following RMX failure to connect to the NTP servers.	13266 VNGFE-2312
19	General	NTP failure message remained after "Socket reconnect (board id: 5)" procedure.	13247/13331 VNGFE-2336
20	General	Core dump occurs and endpoints cannot move from the EQ to the destination Ad Hoc conference created when: • The RMX is configured to Fixed Resource Capacity and all resources are set to CIF/VSW • The system flag ENABLE_H239=NO.	12712/ 12713/13332 VNGFE-2359
21	General	Insufficient resources indication and a Major alarm are displayed when the MPM card did not complete the startup process and could not be recognized by the system.	13335 VNGFE-2320
22	General	After the upgrade to v4.1.1.19, newly created Meeting Rooms cannot be used, but existing Meeting Rooms work successfully	13351 VNGFE-2452
23	General	Card recovery process does not work.	13185 VNGFE-2414
24	General	On a PC with Vista OS, the RMX Manager application cannot be installed.	12195
25	General	In the Hardware Monitoring, statistics are not displayed when monitoring the LAN	12298
26	General	A "$" in the password of an RMX Version 3.0 or 4.0 account prevents access to Hardware Monitor and generates an error when user tries to access the hardware	10341/ 1992

Table 7   *Corrections Between Version 4.5.0.F and Version 5.1.0G (Continued)*

No	Category	Description	ID/ VNGR#
27	General	The Operator and Chairperson are able to delete a participant from the address book when they are not authorized to do so.	9930/ 9931
28	General	On an RMX with two MPM+80 cards installed, when running a 4Mbps conference with a maximum number of participants, video artifacts and pixels may appear.	11337
29	General	The space character cannot be used in the Meeting Room *Routing Name* as it conflicts the SIP dial in standards. If the Routing Name is taken from the *Display Name* field, the space character cannot be used in the *Display Name*.	11353
30	Interoperability	Some HDX endpoints connect at 4SIF resolution even if line rate is 1 Mb.	11697
31	Interoperability	In a conference with a line rate of 1920Kpbs, LPR and AES enabled, H.320 Tandberg MXP dial-in participants cannot connect and an assert appears.	12069
32	Interoperability	When connecting a Tandberg MXP ISDN endpoint to an encrypted conference, loud buzzing noises occur.	11962
33	Interoperability	When an DMA Gateway places dial-in audio calls through an RMX Gateway (version older than 4.1.1), the audio calls cannot connect at the destination RMX installed with version 4.1.1.	11959
34	Interoperability	In a CP conference with a line rate of 384Kbps, when 2 HDX and one VSX endpoints are connected, the VSX receives bad video.	11609
35	Interoperability	Green artifacts appear when a LifeSize Room 200 endpoint connects to a HD Video Switching Meeting Room at a line rate of 1024Kbps.	13338/ VNGFE-2309
36	Interoperability	The video displayed on the VSX endpoint is distorted (stretched), when two endpoints (VSX 7000 and HDX 8000) remain in a conference that is set to Motion, Auto Layout at line rate of 512 Kbps and the video layout changes to 1x1.	13354 VNGFE-2411
37	Interoperability	After MCU reset performed from Hardware Monitor, no audio could be heard when participants were routed via DMA to a conference running on RMX 4000.	13194/ VNGFE-2406
38	Interoperability	No Content is sent or received by the ISDN endpoint when connecting through the RMX GW to a Virtual Room managed by the DMA (version 4.1.1.1_Build_15_SP_2) running on the RMX.	13405/ VNGFE-2468
39	Interoperability	Polycom audio IP endpoints experience various problems when they attempt to call into DMA conferences.	13507/ DMA-385

Table 7   *Corrections Between Version 4.5.0.F and Version 5.1.0G (Continued)*

No	Category	Description	ID/ VNGR#
40	Interoperability	Cannot dial out from a conference running on RMX 2000 version 5.0 to Avaya 1XC (version CM 5.2 and 6.0) and Polycom endpoints.	13632 AVA-1038
41	Interoperability	PictureTel Concorde 4500 ZX endpoint connects to a conference as Secondary (no video) when using ISDN and H.261 capabilities.	9721
42	Interoperability	Frozen Video on VSX6000 and V500 in CP session set to sharpness	11412
43	Interoperability	When endpoints connect to a conference running on the RMX through the DMA, the endpoints will see full screen (1x1) layout and not the conference layout.	11508
44	Interoperability	When using an RMX MCU and a Codian MCU together, each with one ISDN endpoint connected, the endpoint connected to the Codian MCU displays a horizontally stretched picture.	11753
45	Interoperability	Can't connect Sony PCS-1600s over ISDN	11672/ 2219
46	Interoperability	An Ipower v6.2.0.1208 endpoint connecting to an RMX with Siren 14 or G722.1 audio algorithm receives garbled / chopped audio.	11854/ 2258
47	Interoperability	RMX audio is muted or garbled when dialing from PVX endpoints to other endpoints, via the RMX.	11881/ 2277
48	Interoperability	On an RMX 2000 (ver.3.xx) with an H.323i Power (ver. 6.2) endpoint connected at a 256Kbps line rate, the audio from iPower is garbled.	9396/ 1654
49	Interoperability	Tandberg 1700 and Edge95 MXP SIP endpoints cannot transmit video from conferences set to Auto Layout and when the line rate exceeds 1024 Kbps.	11426
50	IP	Occasionally, problems are encountered with the Gatekeeper and memory. The process recovers seamlessly without effecting the overall experience.	12255
51	IP	Latency is always shown as 0 in the Participant's Connection Status.	11749 VNGFE-2241
52	IP	After definition, the Static Route malfunctions.	12288
53	ISDN	Occasionally, RMX with MPM cards and the audio/ video slider is set to 180 audio has limited inbound audio only calls through ISDN to 46 participants. The 47th participant that connects hear a fast busy tone. This limitation is cleared when the system is reset.	13653/ VNGFE-2224
54	ISDN	No Voice Activated Switching when connecting to an ISDN Video participant	11392/ 2024

Table 7   Corrections Between Version 4.5.0.F and Version 5.1.0G (Continued)

No	Category	Description	ID/ VNGR#
55	ISDN/Gateway	Content is not sent from an IP HDX endpoint to an ISDN VSX endpoint via the RMX 2000 gateway when connecting at a line rate of 256 Kbps and the Gateway Profile is set to 'Motion'.	13561/ VNGFE-2489
56	IVR	A conference with a 1920Kbps Line Rate and IVR Service that includes a Welcome Slide, both the Welcome Slide and Video are partially blacked out.	12021/12031
57	IVR	IVR Roll Call Tone is replaced by a recorded participant name due to overwriting the tone *.wav file by the recorded file.	12564 VNGFE-2350
58	Partners - Microsoft	After the .pfx file is installed, the RMX has to be reset in order for it to register to the OCS server and to enable SIP calls. Initiate the Reset from the Hardware Monitor list as no prompt is displayed.	11516
59	Partners - Micro-soft	After the .pfx file is installed, the RMX has to be reset in order for it to register to the OCS server and to enable SIP calls. Initiate the Reset from the Hardware Monitor list as no prompt is displayed.	11516
60	Recording	Recording links on RMX 4.0 do not support AES encryption, although the RSS v4.0 and above have an AES encryption option	11664/ 2186
61	Reservations	An error message is displayed when checking the properties of a reservation in the Calendar view for the first time and the ISDN/PSTN dial in option is disabled for the reservation.	11046 VNGFE-2286
62	Reservations	When an on-going conference duration is set to one minute and auto-extend enabled with an ISDN dial in number, the RMX may not detect an ISDN dial-in No. conflict when placing a reservation on the bridge with an identical ISDN number. In case of a dial-in number conflict, incoming calls are routed to the on-going conference and not to the reserved meeting.	11635
63	Resource Capacity	When the Resource Capacity Mode is set to Flexible and the Port Configuration slider is moved, an incorrect message displays requesting that the RMX be reset.	10884
64	RMX Manager	Cannot install the RMX Manager application from RMX 4000.	12718/ VNGBE-727/ 825
65	RTM ISDN	During an ongoing conference, connection with the RTM ISDN card is lost, causing the ISDN participant to disconnect from the conference, and hardware reset was required to restore the connection with the card.	12975/ VNGFE-2378

Table 7   *Corrections Between Version 4.5.0.F and Version 5.1.0G (Continued)*

No	Category	Description	ID/ VNGR#
66	Security	Plugging Keyboard to USB port and resetting the RMX has the same effect as inserting disk-on-key containing RestoreFactorySecurityDefaults.txt file) The exits Secured Communications Mode (from HTTPS to HTTP).	19992
67	SIP	Occasionally, when a dial-in SIP participant accesses the Entry Queue, the participant connection fails even though the participant entered the correct conference ID.	12017
68	SIP	When trying to connect SIP participant thru external API application, when the URI and IP address fields are switched (the IP address is left empty and the URI is set to the IP address), the endpoint will disconnect.	11971
69	SIP	The maximum number of Meeting Rooms, Entry Queues, SIP Factories and on-going conferences that can be registered to the Proxy, is limited to 100.	11949/11923
70	SIP	The error message ""Network does not have enough resources to complete your call. Try calling at a lower rate" is displayed when two SIP (CMAD) participants dial in to the conference at the same time.	13308
71	SIP	Cannot dial out to a SIP endpoint.	13384/13657 VNGFE-2450
72	Upgrade	After upgrading from version 4.1.1.19 to version 5.0, and the RMX was configured to work with CMA Address Book, the RMX Login window is not displayed.	13189/ VNGFE-2417
73	Upgrade Procedure	Multiple Resets when upgrading from version 3.x, 4.0x to version 4.1. The upgrade process was improved by: • Adding progress bar for startup. • Improving the download process to the MCU. • Reducing the number of required resets.	
74	Upgrade Procedure	Sometimes after upgrade, the MPM card remained in Reset Mode.	
75	Upgrade Procedure	Sometimes after upgrade, the connection with the RTM IP (switch) is lost.	
76	Video	Site names are not displayed in 4x4 and 1+10 layouts.	11680
77	Video	Sometimes, the video processing units on the MPM cards are not responding and MCU reset is required.	13415/ VNGFE-2460

Table 7   *Corrections Between Version 4.5.0.F and Version 5.1.0G (Continued)*

No	Category	Description	ID/ VNGR#
78	Web Client	After logging-in and out several times in the Web Manager, the UI appears in English instead of French.	12096

Version 7.5.0.J System Limitations

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
1	*Audio*	VNGR-14578	On an RMX with a license for 800 audio only participants, a disconnection cause always occurs after connecting the 767th participant.	V6.0	
2	*Audio*	VNGR-14687	When connecting 800 VOIP using 4 Entry Queues and 396 Ad Hoc conferences, when adding Dial out participants to the conferences they could connect. An MCU error message appears: MCU INTERNAL PROBLEM - 65012.	V6.0	
3	*Audio*	VNGR-15938	RMX 4000 using HDX endpoints in 2048Kpbs HD Video Switching conference using Siren22Stereo exceeds conference bit rate by sending data to endpoints at 2112kpbs.	V7.0	
4	*Audio*	VNGR-16272	RMX 4000 using HDX endpoints in 2048Kpbs HD Video Switching conference using Siren22Stereo exceeds conference bit rate by sending data to endpoints at 2112kpbs.	V7.0	
5	*Audio*	VNGR-16794	On RMX 4000 with MPM+, G.728 endpoint isn't declared 1st endpoint in conference at 96kbps.	V7.0	
6	*Audio*	VNGR-16798	Medium volume horn-like sound heard for several minutes on HDX4000 endpoint connected to RMX 4000 with MPM+ via DMA Meeting Room.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
7	*Audio*	VNGR-16919	On RMX with MPMx using H.323 with HDX endpoint, sites do receive Siren14 instead of Siren22 Stereo audio algorithm 6Mbps VSW conferences.	V7.0	
8	*Audio*	VNGR-16935	On RMX 1500, running 384kbps conference, an endpoint connected with ##FORCE_MEDIA_ASIREN14_24K or ##FORCE_MEDIA_ASIREN14_32K connects with a SIREN14_48K audio algorithm. An endpoint connected without force connects using G.711 audio algorithm.	V7.0	
9	*Audio*	VNGR-	Received audio volume of PSTN audio-only participants is approximately three times lower than that received by video participants.	V7.0	
10	*Audio*	VNGR-17070	On an RMX 4000 with MPM+ cards, when running a 512 Kbps conference with mixed HDX 8000 and VSX 3000 endpoints, audio cuts ON and OFF.	V7.0	
11	*Audio*	VNGR-17320	When dialing in from several endpoints to a Meeting Room started by the DMA, audio was lost for several seconds on the HDX9006 endpoint.	V7.0	
12	*Audio*	VNGR-17471	Loss of audio for 2-3 seconds or bursts of static noise on HDX6000 endpoint in calls dialed via DMA to RMX4000 running V7.0.1.16 with, 4*MPM+80 cards	V7.0.1	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
13	*Audio*	VNGR-17616	HDX H.323 endpoint receives G.722 audio instead of Siren22 (as the SIP endpoints) when connected to a conference running at a line rate of 384kbps on RMX4000 with MPM+ and the CS_ENABLE_EPC flag is set to YES.	V7.0.2	
14	*Calendaring*	VNGR-13686	On the RMX 4000 in a 1080p H.323 Video Switching conference with a line rate of 6Mb, the IVR welcome screen can freeze on the HDX8006 and HDX 9006 endpoints.	V6.0, V5.0.0	
15	*Calendaring*	VNGR-13810	In version 6.0, in the Conference Profiles list, the default Event Mode (COP) profile is not used, and should not be listed.	V6.0	
16	*Cascading*	VNGR-11953	When connecting to a cascaded CP conference with a 768Kpbs line rate and the video quality set to Sharpness, HDX endpoints experience bad video quality.	V5.0.0	
17	*Cascading*	VNGR-16239	Create two 384Kbps cascaded conferences with LPR enabled, when creating the dial-out Master link to the second conference is only partially connected.	V7.0	
18	*CDR*	VNGR-11746	GMT Time Offset is written to the unformatted CDR as 0.	V4.1	
19	*CDR*	VNGR-1569	When the conference termination time is changed, the CDR is not updated.	V1.0.0	
20	*CDR*	VNGR-3011	The Encryption field is missing from the CDR file.	V1.1.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
21	*CDR*	VNGR-9340	When a conference was terminated by an MCU reset, an incorrect status "Ongoing Conference" will be displayed in the CDR List pane.	V4.0.0	
22	*CMA*	VNGR-11543	When creating a conference using the CMA, the Conference Management UI displays the participants as disconnected, even though they are connected.	V4.1	
23	*Content*	VNGR-11491	In a conference with a line rate of 384Kbps, when H.323 participant connect to the conference using FECC, incorrect data is displayed in the Participant Properties - FECC and Content channels of the RMX Web Client. The information is updated correctly once the participant is fully connected.	V4.1	
24	*Content*	VNGR-16203	In a 768 Kbps Meeting Room with LPR, Echo Suppression, Auto layout and Motion enabled when the first to join the Meeting room sends content, the second participant to join views a black screen.	V7.0	
25	*Content*	VNGR-16281	Content sent from HDX (in H.264) is automatically stopped when a second participant that does not support H.264 Content (for example, CMAD that only supports H.263) joins the conference. When the content is sent again, the Content protocol is H.263+ to enable all conference participants to receive content.	V7.0	
26	*Content*	VNGR-16807	Bad audio quality experienced on PVX endpoint while it sends content when connected to RMX 1500.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
27	*Content*	VNGR-16830	In a mixed H.323 & SIP 1152Kbps conference with Video Clarity, Auto Terminate, Sharpness, Echo Suppression, Auto Layout, Gathering and Send content to Legacy endpoints enabled, HDX endpoint's content is fragmented.	V7.0	
28	*Content*	VNGR-17558	Legacy endpoint that connect to a conference in which Content is already sent, and the conference layout is set to Auto Layout the does not see the Legacy Layout and does not receive content.	V7.0.2	
29	*Content*	VNGR-19881	Chroma shift viewed on Legacy endpoints when sending content in a conference running on RMX 2000 with MPMx at a line rate of 512kbps and the Send Content to Legacy Endpoint option enabled.	V7.5	
30	*Content*	VNGR-17671	Content sent from a VSX7000A system. is displayed frozen on the far end VSXs when connected over H.323 to a conference with 9 H323 VSX endpoints running on RMX4000 with the MPM+ at a line rate of 768kbps and LPR, Video Clarity and Send Content To Legacy Endpoint options enabled.	V7.0.2	
31	*Content*	VNGR-17762	Sometimes Content is sent during the gathering phase and is shown through the gathering phase slide background (it is displayed as a layer underneath it) when the Sent Content to Legacy Endpoint option is enabled in a conference running at 384kbps.	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
32	*Content*	VNGR-17729	Video freeze was experienced by many participants when content was sent from a PC to 160 CIF participants connected to a conference running on RMX 2000 with MPM+80 at a line rate of 384kbps and LPR and Encryption options enabled.	V7.0.2	
33	*Diagnostics*	VNGR-16142	On the RMX1500/2000 when running the "Diagnostic - RTM ISDN", test ID 717 RTM TDM FALC1 Diag, the test fails. Reason for the test failure: "RTM Timeout - RTM didn't send Test Completed".	V7.0	
34	*Diagnostics*	VNGR-16742	On an RMX2000 with MPMx_D cards when performing an Power ON Self Test (POST), the MPMx card runs the card monitoring test in an endless loop.	V7.0	
35	*Diagnostics*	VNGR-16754	On an RMX 4000 in the Diagnostic mode when pressing the menu reset button the following message appears: "connection with shelf management is lost, please log in again". You can only exit the Diagnostic mode after physically turning the RMX Off and On.	V7.0	
36	*Diagnostics*	VNGR-18257	Software verification failure is indicated when running diagnostics on RMX 1500 (MPMx card).	V7.0.2	
37	*Encryption*	VNGR-11401	In an encrypted conference, Tandberg MXP endpoints encounter audio problems.	V4.1	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
38	*Encryption*	VNGR-12202	Rarely, in an encrypted conference, H.323 encrypted dial-in and dial-out participants cannot connect and an assert appears (File:EncryptionKeyServer Manager.cpp).	V5.0.0	
39	*Encryption*	VNGR-14840	No video is seen and the Aethra VegaStar Gold endpoint remains connected with a problem when connecting over H320 to an encrypted conference at a line rate of 384Kbps.	V6.0	
40	*Encryption*	VNGR-15256	In a conference with an IVR Service with endpoints, when using DTMF (*71/#71/*88) codes to secure/unsecure the conference there is no text/ icon indication.	V7.0	
41	*FECC*	VNGR-16523	On the RMX 1500 running a mixed H.323 & SIP 384Kbps conference, when connecting an Tandberg SIP endpoint, FECC does not work.	V7.0	
42	*Gateway*	VNGR-15935	In the RMX Web Client, when creating a new gateway profile and setting the Gateway ID to "#1234" then click OK, no confirmation message appears.	V7.0	
43	*Gateway*	VNGR-16562	Gateway sessions are always running in CP mode. If Video Switching is selected in the Profile, the system will change it to CP mode, using the closest possible video settings. However, 60fps may not be supported in CP mode for the selected line rate.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
44	*Gateway*	VNGR-16604	In a Gateway call started from a video endpoint (CMAD or HDX) when other endpoints connect, the endpoint that initiates the call initially views the Gathering slide but then it disappears.	V7.0	
45	*Gateway*	VNGR-16607	When a Gateway call is started from a video endpoint (CMAD or HDX) and endpoints connect to the conference, SIP endpoints view a blurry gathering slide with artifacts.	V7.0	
46	*General*	VNGR-10922	Dial out to participants assigned to a Meeting Room will only start when the dial-in participant who has activated it has completed the connection process and the Meeting Room has become an ongoing conference.	V4.1	
47	*General*	VNGR-11324	When moving many participants simultaneously from one conference to the other (both with a line rate of 1920 Kbps), a number of HDX8000 endpoints connect secondary. When trying to disconnect and reconnect the participants connected as Secondary, an MCU Internal error 32122 is displayed.	V4.1	
48	*General*	VNGR-11383	When updating the Profile assigned to a Conference Template, changes are not applied when the conference becomes ongoing.	V4.1	
49	*General*	VNGR-11422	When the RMX is set to Flexible Allocation Mode and more than 14 endpoints are connected to a single MPM+80 card in line rates above 2Mbps, video artifacts may appear.	V4.1	Change the resource Allocation Mode to Fixed Mode.

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
50	*General*	VNGR-11701	Sometimes a system error "SOFTWARE_ASSERT_FAILURE" appears when the RMX is running under load (repetitive connecting and disconnecting participants).	V4.5	
51	*General*	VNGR-11883	After software upgrade, it is necessary to close and reopen Internet explorer.	V5.0.0	
52	*General*	VNGR-11987	When upgrading from V4.0.3 to V5.0, after inserting the activation key an invalid key message appears.	V5.0.0	Logout and login to the web browser or reopen the Internet Explorer.
53	*General*	VNGR-12033	Rarely a system error (BridgePartyVideoOut.cpp, Line:1458, Code:1701.; DEBUG-ASSERT:) is written to the log file if a change is made to the conference layout while participants are disconnecting.	V5.0.0	
54	*General*	VNGR-12100	Occasionally, after upgrading to version 5.0 (from 4.0.3, 4.1.0, 4.1.1), the soft reset fails.	V5.0.0	First try to reset from the SHM if possible. Otherwise hard reset the system.
55	*General*	VNGR-12181	Sometimes an assert may appear when terminating a conference while running 10 conferences at a line rate of 768Kbps and changing the layout for H.323 & SIP participants.	V4.6	
56	*General*	VNGR-12240	Endpoints are disconnected after extended time period (8 hrs +) when all MPM+ resources are used. Error message is displayed: "Unit not responding".	V5.0.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
57	*General*	VNGR-14062	On a fully loaded RMX 4000, endpoint may disconnects with Call Disconnection Cause stated as "MCU internal problem - 11122".	V6.0	
58	*General*	VNGR-14151	A Shelf Voltage problem is always displayed in the System Alerts pane regardless of the actual status.	V6.0	
59	*General*	VNGR-14159	Operator assistance function is blocked when the TelePresence mode is enabled.	V6.0	
60	*General*	VNGR-14624	After changing the conference profile assigned to a conference template that includes participants, some of these participant are randomly deleted from the conference template.	V7.0	
61	*General*	VNGR-14667	When defining a New Profile in the Video Settings tab and selecting a Layout, in the Conference Profiles list there is no indication of the selected layout and the layout icon is missing.	V6.0	
62	*General*	VNGR-14688	When a conference is deleted in the RMX Manager, conference participants are not deleted in the participants list.	V6.0	
63	*General*	VNGR-14767	H.323 party disconnect due to MCU Internal Problem 32212.	V6.0	
64	*General*	VNGR-15320	Saving to a Conference Template a conference in which the Message Overlay is enabled, automatically enables the message overlay option in the conference that is started from this template.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
65	*General*	VNGR-15324	o When monitoring a CP conference with 5 or more endpoints from 5 Web Client sessions on separate workstations, Video Previews can be opened from 4 workstations. Attempting to open a fifth Video Preview causes an error "Failed to Preview Video: Failure Status" instead of "The Preview cannot be displayed. The maximum number of previews per MCU has been reached."	V7.0	
66	*General*	VNGR-15366	Sometimes when Restore Factory Defaults is performed, the active alarm "CPU slot ID not identified- McuMngrCPU board id was not received from ShelfManager" is displayed.	V7.0	
67	*General*	VNGR-15523	Primary and Secondary dial in numbers entered in the Polycom Conferencing Add-in to Microsoft Outlook are always displayed on the Gathering slide (during the gathering phase) for reference, even if the participant connected using the invitation link.	V6.0	
68	*General*	VNGR-15553	On an RMX 2000 with MPMx cards, during startup a list of error appears.	V7.0	
69	*General*	VNGR-15554	Numerous missing Japanese translations in the RMX Web Client.	V7.0	
70	*General*	VNGR-15637	After creating a conference template with 6 participants, when adding and removing participants to a conference the template does not update.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
71	*General*	VNGR-15718	Incorrect disconnection cause after pulling LAN cable from RMX. The endpoints reports that the "call close normal".	V7.0	
72	*General*	VNGR-15737	In the Resolution Configuration Slider, the CIF30 slider is absent from the UI.	V7.0	
73	*General*	VNGR-15746	When downloading and installing version 7.0, the Download window lists version 6.0.	V7.0	
74	*General*	VNGR-15750	In a conference set to 512kbps with Auto Layout enabled, when starting PCM from several endpoints, - you will receive an Message Overlay: "no available PCM resources". The message overlay cannot be closed.	V7.0	
75	*General*	VNGR-15755	During an active Telepresence conference, click the Video Settings tab, the "Telepresence Mode enabled" check box appears when it should not.	V7.0	
76	*General*	VNGR-15837	In 768Kbps conference set to AES, CP, Full Layout and two HDXs Chairperson, when the SIP HDX invokes PCM Camera Control only segmented video can be seen.	V7.0	
77	*General*	VNGR-15953	When copying and pasting conferences based on a Profile, the pasted conference is added to conference templates.	V7.0	
78	*General*	VNGR-16044	After downloading and opening an auditor file of the MPMx, the MPMx name appears as MPM_PLUS.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
79	*General*	VNGR-16103	After running diagnostics on the RMX, LED functionality is not documented.	V7.0	
80	*General*	VNGR-16120	Saving to a Conference Template a conference in which the Message Overlay is enabled, automatically enables the message overlay option in the conference that is started from this template.	V7.0	
81	*General*	VNGR-16170	On an RMX 4000, endpoints using the layout 1+7, endpoints are not in the proper location.	V7.0	
82	*General*	VNGR-16230	In a Meeting Room with five participants all endpoints receive periods of frozen audio and video.	V7.0	
83	*General*	VNGR-16237	Connect to an RMX as Operator using the RMX Manager. Then connect an Administrator to same RMX the following message appears: "cannot login to MCU x.x.x.x with the user name and password entered".	V7.0	
84	*General*	VNGR-16283	In a conference with a few participants, when opening the video preview pane and previewing the next participant without closing the pane, the pane becomes minimized, and does not show video of the next participant.	V7.0	
85	*General*	VNGR-16296	The Host name is not defined in the Fast Configuration Wizard during the initial system configuration. Therefore when trying to configure either the "Control" or the "Shelf" IP address (or both), the error message "Invalid Host Name" is displayed when clicking OK.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
86	*General*	VNGR-16338	In a 4MB HD CP conference set to 720p with 3 participants, 1 endpoint disconnected due to the following message: "MCU internal problem".	V7.0	
87	*General*	VNGR-16377	On an RMX with MPM+ card, when starting a VSW conference from the Profile, you can select 6144 Kbps as the line rate.	V7.0	
88	*General*	VNGR-16427	On RMX 1500 with two conferences running and Legacy Content enabled, line artifacts are displayed in the middle of the CMAD screen after it is disconnected from the first and reconnected to the second conference.	V7.0	
89	*General*	VNGR-16466	On RMX 2000 with MPM, "MCU Internal Problem - 32112" occurs during mini-load smoke on MPM when 20 video participants are connected at 384kbps.	V7.0	
90	*General*	VNGR-16471	Extraneous MCMS version number is displayed in the detailed faults list.	V7.0	
91	*General*	VNGR-17099	Extraneous "Total Number of Event Mode Resources" field is displayed in the System Information properties box.		
92	*General*	VNGR-16529	After Restoring Factory Defaults on the RMX and defining the IP Network Service, after RMX restart the MCU Host Name parameter appears empty in the "Management Network - DNS" tab.	V7.0	
93	*General*	VNGR-16560	After log-in to the RMX 1500 Web Client, a Microsoft .NET Framework error message appears.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
94	*General*	VNGR-16581	On an RMX 2000 & MPM+ cards, running an 384Kbps CIF conference, with Auto Terminate, Encryption, LPR, Echo Suppression, Sharpness and Same Layout enabled, when sending content from an HDX to 160 other endpoints, an "Software assert failure" appeared.	V7.0	
95	*General*	VNGR-16582	On an RMX 2000 & MPM+ cards, running an 384Kbps CIF conference, with Auto Terminate, Encryption, LPR, Echo Suppression, Sharpness and Same Layout enabled, when sending content from an HDX to 160 other endpoints, an "Software assert failure" appeared.	V7.0	
96	*General*	VNGR-16600	On an RMX2000 & MPMx card running a mixed H.323 & SIP 1920Kbps conference with AES, Sharpness and Gathering enabled, when the RMX dials-out to 10 endpoints, the border layouts are "speckled" and miss their edges.	V7.0	
97	*General*	VNGR-16610	The Column width displayed in Web Client and in the RMX Manager UI need to be made broader.	V5.0.1, V5.0.0, V4.6.1, V6.0, V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
98	*General*	VNGR-16621	Run two conferences that support Content for Legacy Endpoints, connect all types of endpoints to each conference and then send content from a non Legacy endpoint to each conference. The conference layout on the Legacy endpoint is changed to the flag's CP_LAYOUT_1P4VER configuration, the default layout. Move one legacy EP to the second conference - the layout of it changes to conference layout	V7.0	
99	*General*	VNGR-16624	In the RMX Manager, when attempting to upgrade two RMX simultaneously, the Install Software window only appears for one RMX, when you should view both.	V7.0	
100	*General*	VNGR-16625	Sometimes when upgrading to version 7.0 and resetting the RMX 2000, an active alarm "CPU slot ID not identified - McuMngrCPU board id was not received from ShelfManager" is displayed.	V7.0	
101	*General*	VNGR-16745	In the RMX manager 7.0, the "new conference" icon suddenly appears in the conferences properties window.	V7.0	
102	*General*	VNGR-16751	When creating a second conference with a display name that is already used by another conferencing entity, the conference properties dialog box re-opens with a redundant check box next to the routing name field.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
103	*General*	VNGR-16793	On an RMX 2000 with MPM+, start an 4096Kbps 1x1 Layout conference from a template with Encryption, LPR, Auto Termination, Sharpness, Same Layout, Audio Clarity enabled, an "mcu internal problem: 32212" message appears in conference properties - connection status tab.	V7.0	
104	*General*	VNGR-16861	On an RMX 2000 with 2 MPM+80 and 2 RTM ISDN Cards (5 T1/PRI connecting to each RTM ISDN card), only 70 CIF dial-out endpoints can connect to the 128 Kbps conference.	V7.0	
105	*General*	VNGR-16865	MCU INTERNAL fault received on RMX 1500: "UnitId 20 (board 1) didn't return ACK for H323_RTP_UPDATE_PORT_OPEN_CHANNEL_REQ."	V7.0	
106	*General*	VNGR-16871	In 384kbps conference on RMX with MPMx, HDX endpoint's "Used Call Rate" is approximately 100kbps lower than expected.	V7.0	
107	*General*	VNGR-16890	Log Analyzer output from RMX 1500/2000 with MPMx contains numerous CRT ART errors.	V7.0	
108	*General*	VNGR-16934	When a H.323 call is released without lobby conn_id parameter, call memory is possibly not released.	V7.0	
109	*General*	VNGR-17009	On both the RMX 2000/4000 when running conference on an MPMx card with a minimum of 8 participants and viewing content, the conference terminates due an MPMx disconnection.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
110	*General*	VNGR-17436	Unit recovery of unit 14, board 1 occurred.	V7.0.1	
111	*General*	VNGR-17496	DSP recovery and asserts occur, endpoints are disconnected or lose both audio and video on RMX4000 running V7.0.1.16 with 4*MPM+80 cards.	V7.0.1	
112	*General*	VNGR-17517	"Insufficient resources" with "Power off problem" errors occur when 15 HDX 8006 and 10 HDX 9004 that are connected to a conference at a line rate of 4096kbps are muted and unmuted individually and then the conference layout is changed.	V7.0.2	
113	*General*	VNGR-17520	In MPMx Card Configuration Mode, the High Profile Sliders in the Resolution Configuration dialog box are set to the minimum and do not show the actual values for the predefined Resolution Configurations.	V7.0.2	
114	*General*	VNGR-17587	Several participants are deleted from a conference template when editing the conference template name.	V7.0.2	
115	*General*	VNGR-17714	Occasionally, RMX 4000 with MPM+ automatically resets when running conferences. The system displays the Active Alarm: NEW_VERSION_INSTALLED: A new version was installed. Reset the MCU, although a new version was not installed.	V7.0.2	
116	*General*	VNGR-17724	After Comprehensive Restore to Factory Defaults, an active alarm displayed, indicating voltage problem on MPM-f - card.	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
117	*General*	VNGR-17791	DTMF Tones (Click&View) are heard by all conference participants in a conference running on RMX 2000 with MPMx.	V7.0.2	
118	*General*	VNGR-17843	HDX H323 endpoints are unable to remain connected to a CP conference running on RMX1500 at a line rate of 1920kbps with LPR, Video Clarity and Send Content to Legacy Endpoint options enabled. The disconnect status displays MCU internal problem 32212.	V7.0.2	
119	*General*	VNGR-18167	When using a conference Profile set to VSW 1080p at line rate of 6MB, the conference is started at a line rate of 4MB instead.	V7.0.2	
120	*General*	VNGR-18349	Following a Comprehensive Restore to Factory Defaults of RMX 2000, the CDR file containing 1000 CDR logs cannot be restored from the Backed up configuration.	V7.0.2	
121	*General*	VNGR-3824	The Click & View menu doesn't appear in 64 Kbps calls.	V1.1.0	Use the RMX Web Client.
122	*General*	VNGR-9729	When moving from MPM+ to MPM mode (with only MPM cards installed in the MCU), the Card Configuration Mode, indicated in the System Information dialog box, remains in MPM+ Mode.	V4.0.0	Logout and then login to the RMX Web Client.
123	*General*	VNGR-9803	When using the restore to factory defaults, after inserting the Activation key, the system requires a reset when the reset is not required.	V4.0.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
124	*General*	VNGR-19722	Audio card fails to initialize during startup on RMX4000 resulting in no utilizable unit for audio controller.	V7.5	Reset the RMX.
125	*H.323*	VNGR-11810	The following assert may appear when H.323 participant connects to a 2 Mb Continuous Presence conference: File:AuditorApi.cpp, Line:112, Code:1.; ASSERT:Audit_free_Data_is_too_long_20882,_max_is_20480data_size_is_:_20882	V5.0.0	
126	*Hardware*	VNGR-9571	In D-type chassis, when hot-swapping an MPM card, unit failure may occur.	V4.0.0	Reset the MCU
127	*Hardware*	VNGR-14550	On the MPM+, experience problems with DSP#1 during load testing.	V7.0	
128	*Hardware*	VNGR-16058	After upgrading RMX4000, an error message appears: "No RTM-LAN or RTM-ISDN installed" on slots 13, 14, 15". In fact no RTM-ISDN card is installed in slot 13.	V7.0	
129	*Hardware*	VNGR-16474	On RMX 1500 with MPMx-S, MCU internal problem 32112 occurs repeatedly in 2Mbps VSW or CP conference using HDX 8000 endpoint. Problem did not occur after reset.	V7.0	
130	*Hardware*	VNGR-16537	On the RMX 1500 when the RMX is in a "Diagnostic Mode" the listed slot numbers of the modules are incorrect.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
131	*Hardware*	VNGR-16785	Run 8 512Kbps conferences and connect to each conference 2 H.323, 2 SIP, 1 ISDN, 1 PSTN & 1 VOIP endpoints, change the conference layout on each, when terminating the conferences an "MCU Internal Problem 50020" occurred on the MPMx cards.	V7.0	
132	*Hardware*	VNGR-16936	On an RMX 4000 when viewing the Signaling Monitor window, the Active Alarms pane shows no link between Fabric Switch Module and MPMx card in slot 1.	V7.0	
133	*Hardware*	VNGR-16945	On the RMX2000 and RMX4000, when performing diagnostics using the Power on Self Tests (POST) you cannot access the Shelf Manager.	V7.0	
134	*Hardware*	VNGR-17001	MPMx card remains in startup mode instead of Major state after restoring the RMX to factory defaults and without configuring the IP address of the media card(s) in the Fast Configuration Wizard.	V7.0.1	
135	*Hardware*	VNGR-17157	DSP did not automatically recover after failure.	V7.0.1	
136	*Hardware*	VNGR-17194	Board recovery failure occurs after all units on board 2 stop sending data after 3 recovery attempts on RMX2000 running V7.0.0.162 with MPMx cards.	V7.0	
137	*Hardware*	VNGR-17851	Sometimes connection with RTM ISDN is lost.	V7.0.2	
138	*Hardware*	VNGR-17869	When inserting a Control Unit in Slot 4, in Hardware Monitor it is shown as inserted in slot 3	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
139	*Hardware*	VNGR-17881	RTM IP does not reconnect to logger port.	V7.0.2	
140		VNGR-19038	On an RMX 2000/4000 with Ultra Secure Mode/ Secure Communication enabled, after a system restart; the system date sometimes reverts back to a previous date or incorrect date.	7.5	
141	*HD*	VNGR-16780	During VSW conference at 720p60p resolution using direct connections or via DMA, endpoints display only their own video.	V7.0	
142	*HD*	VNGR-3089	In HD Video Switching conferences, Tandberg endpoints may connect as Secondary when HD frame rate capabilities are less than 7.5 frames per second.	V1.1.0	Create a CP conference
143	*Interoperability*	VNGR-10849	A black screen may appear in the following instances: * On HDX8000 HD Hardware version B endpoints when the conference line rate is set in the range of 256-768 Kbps. (The Hardware version can be found on the HDX endpoint's System Information page.) * On HDX SD endpoints using the PAL mode when the conference line rate is set above 128 Kbps.	V4.1	(1) Upgrade to HDX software version 2.5.0.5 (2) Use conference line rates below 256 or above 768 Kbps. (3) Disable the IVR Welcome slide and avoid using a 1x1 Video Layout.
144	*Interoperability*	VNGR-10989	In a ISDN dial-in conference with a line rate of 384 Kbps, Tandberg MXP ISDN endpoints cannot view content.	V4.1	
145	*Interoperability*	VNGR-11341	During H.320 calls, Lip Sync issues occur when content is being sent.	V4.1	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
146	*Interoperability*	VNGR-11489	In a conference running at a line rate of 384 Kbps, when HDX 8006 endpoint that sends Content is moved to another conference, Content is still viewed for a number of seconds on the HDX.	V4.1	
147	*Interoperability*	VNGR-11563	Legacy endpoints occasionally cannot switch to Content when Content switched from H,264 to H.263.	V4.1	
148	*Interoperability*	VNGR-11767	In a 6 Mb, Video Switched conference, HDX endpoints that declare 2 Mb capability may only connect at a line rate of 896 Kbps after 30 seconds.	V4.1.1	
149	*Interoperability*	VNGR-11798	When Tandberg C20 endpoint sends Content, the far end indicates that Content is being received but received Content is black.	V5.0.0	
150	*Interoperability*	VNGR-11830	Sony XG80 endpoint cannot send Content in H.323 384 Kbps call.	V6.0	
151	*Interoperability*	VNGR-11920	In a 4 Mb RPX conference with LPR enabled, video-out bit rate decreases to 128 Kbps due to packet loss and does not increase.	V5.0.0	
152	*Interoperability*	VNGR-11963	In a conference running at a line rate of 384Kbps with AES, LPR and Video Clarity enabled, HDX ISDN participants connect with SIF resolution while HDX IP endpoints connect using a 4SIF resolution.	V5.0.0	

#	Category	Key	Description	Detected in Version	Workaround
153	*Interoperability*	VNGR-12177	In a conference with AES, LPR and Video Clarity enabled, H.320 Tandberg MXP endpoints connect with resolution of 960x720, while identical H.323 MXP endpoints connect with resolution of 720p.	V5.0.0	
154	*Interoperability*	VNGR-12178	In a conference with AES, LPR and Video Clarity enabled, H.320 HDX8006/ HDX9004 endpoints send Content in H.263 only.	V5.0.0	
155	*Interoperability*	VNGR-12266	Tandberg MXP endpoint receives ghosted video from HDX9004 endpoint during H.323 conference.	V5.0.0	
156	*Interoperability*	VNGR-12355	DST K60 endpoint receives tiled video from HDX9004 endpoint during H.323 conference.	V5.0.0	Set the system flag SEND_WIDE_ RES_TO_IP to NO to force the system to send 4CIF.
157	*Interoperability*	VNGR-12369	Tandberg C20 endpoint periodically displays fast updates in HD1080p conferences.	V5.0.0	
158	*Interoperability*	VNGR-12372	Tandberg 6000 E and B series, H.320 endpoints do not connect to conferences when encryption is enabled.	V5.0.0	
159	*Interoperability*	VNGR-12373	HDX endpoint connected via H.320 does not receive Content from Tandberg MXP endpoint connected via H.323.	V5.0.0	
160	*Interoperability*	VNGR-12415	In a conference running at a line rate of 1728 Kbps set to Same Layout, when PVX/VSX7000 participants connect in CIF264/263, an error message appears.	V4.6	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
161	*Interoperability*	VNGR-14047	Artifacts appear on LifeSize _RM1_4.5.1(15) endpoint connected via SIP or H.323 to a 2Mbps conference with Video Quality set to "Sharpness" running on the RMX 2000 in MPM mode. The LifeSize endpoint is using 4SIF 30 resolution while Polycom endpoints are using 720*400 resolution.	V6.0	
162	*Interoperability*	VNGR-14780	RMX4000 using 4Mb, Same Layout, Sharpness, Video Clarity in profile and Entry Queue becomes inaccessible when called via an Entry Queue from H.323 LifeSize endpoint.	V6.0	
163	*Interoperability*	VNGR-15096	In a 384Kbps conference with no LPR, when connecting HDX 8000, PVX endpoints the lower segment of the welcome's slide is missing/smudged.	V7.0	
164	*Interoperability*	VNGR-15129	In a conference set to a line rate of 4096kbps with Sharpness, 1+5 layout, with a number of endpoints present, when a H.323 HD720p30 Tandberg 1700MXP endpoint dial-outs, Video In & Out freeze.	V7.0	
165	*Interoperability*	VNGR-15281	Aethra VegaStar Gold endpoint, when connecting via ISDN to 384kbps conference creates CDR Event - Participant status "Connected with problem".	V7.0	
166	*Interoperability*	VNGR-15649	In a continuously running conference, after disconnected two HDX7000 and VSX7000 endpoints, the HDX4000 endpoint's video freezes.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
167	*Interoperability*	VNGR-15789	RMX4000 using 4Mb, Same Layout, Sharpness, Video Clarity in profile and Entry Queue becomes inaccessible when called via an Entry Queue from H.323 LifeSize endpoint.	V6.0	
168	*Interoperability*	VNGR-15906	In a 384Kbps conference with no IVR and resources set to a Fixed Mode when connecting SIP/H.323 HDX & PV dial-in and dial-out endpoints, the SIP receives bad video.	V7.0	
169	*Interoperability*	VNGR-15937	In a conference with HDX8006A, HDX8006B, HDX9000, VSX7000 and ViewStation512 endpoints, the site names of the ViewStation endpoints are switched.	V7.0	
170	*Interoperability*	VNGR-15939	In a "Fixed resource Capacity" mode, Legacy endpoints can still receive content when they should not.	V7.0	
171	*Interoperability*	VNGR-16192	In 2MB Conference with Sharpness enabled when connecting RPX 400, TPX 306 and RPX 200 endpoints not all endpoints can connect.	V7.0	
172	*Interoperability*	VNGR-16194	On an RMX4000 version 7.0, with four VVX 1500s and an 1 HDX 9000 endpoints connected on multiple occasions loss of video and audio for several seconds.	V7.0	
173	*Interoperability*	VNGR-16297	CMAD receives distorted video while calling to RMX.	V7.0	
174	*Interoperability*	VNGR-16322	On an RMX 2000 running a 1920 Kbps Telepresence conference, endpoints have the top part of their video screen cropped off.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
175	*Interoperability*	VNGR-16363	On the RMX2000 with an MPMx card, when starting a new a 2MB conference, Ipower endpoints take a long time to connect.	V7.0	
176	*Interoperability*	VNGR-16378	In a SD conference (1024 resolution) with motion, auto layout enabled, when connecting HDX and dial in from Life Size endpoint, the endpoints do not connect in SD with 60 FPS as required.	V7.0	
177	*Interoperability*	VNGR-16383	On the RMX2000 with an MPMx card in a 512Kbps conference with High Profile, Gathering, IVR, Echo Suppression enabled and resources set to a Flexible Mode, when dialing-out using H.261, connection problems are encountered in VSX endpoints after about 10 seconds.	V7.0	
178	*Interoperability*	VNGR-16387	On an RMX2000 with the MPM+ card, when connecting with an HDX9000 endpoint to the Entry Queue using a line rate of 384Kbps, the IVR slide blinks.	V7.0	
179	*Interoperability*	VNGR-16390	In a 768Kbps Telepresence conference when connecting to a TPX using a 1x7 layout, the HDX8000 video looks elongated in the large cell.	V7.0	
180	*Interoperability*	VNGR-16408	In a 4096Kbps conference with Auto Layout enabled, when dialing out to 3 HDX and 3 VSX endpoints, video freezing occurs.	V7.0	
181	*Interoperability*	VNGR-16506	Lip sync is noticeable on HDX 7000 rev. B that dials into a conference running at a line rate of 1Mbps.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
182	*Interoperability*	VNGR-16519	In an 512Kbps CP conference with AES and Sharpness enabled, when Dial-in endpoints view the Gathering slide the CMAD video freezes.	V7.0	
183	*Interoperability*	VNGR-16595	On an RMX 4000 & MPM+ cards, running an 1920Kbps conference with Video Clarity, Auto Terminate, Video Quality, Sharpness, Encryption, LPR, Echo Suppression, Auto Layout, Gathering and Content for Legacy Endpoints enabled, when connecting 20 HDX, Tandberg 17000 and edge95 MXP & 3 Tandberg C series endpoints the MFA card error occurs.	V7.0	
184	*Interoperability*	VNGR-16599	On an RMX 2000 in a H.261 video conference, when a Tandberg MXP6000 connects using H.261 there is no video.	V7.0	
185	*Interoperability*	VNGR-16643	A conference started from the default video conference, an H.320 Sony PCS-G50 endpoint transits the Entry Queue and when accessing the conference it connects with no video.	V7.0	
186	*Interoperability*	VNGR-16644	In a conference started from the default conference profile, when the RMX dials-out to the H.323 iPower 9000 endpoint, it views the IVR welcome screen for about 40 seconds before viewing conference video.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
187	*Interoperability*	VNGR-16646	In a conference started from the default Profile, when the RMX dials-out to an H.320 iPower 9000 endpoint, the endpoint's video layout is shifted to the bottom right of the monitor with black borders on the left and top of the screen.	V7.0	
188	*Interoperability*	VNGR-16650	In a 384Kbps SIP conference with Auto Layout, Sharpness, Video Clarity, Gathering and Send Content to Legacy Endpoints enabled, when the RMX blast dial-out all types of endpoints, the VSX7000 and VSX8000 sites display video stills throughout the conference.	V7.0	
189	*Interoperability*	VNGR-16735	LifeSize endpoints transmits CIF instead of HD 720p resolution in a SIP1920Kbps conference call located on an MPMx card.	V7.0	
190	*Interoperability*	VNGR-16737	On an RMX 4000 with an MPM+ card, LifeSize does not transmitting or receiving video during a SIP 1920Kbps conference call.	V7.0	
191	*Interoperability*	VNGR-16776	Undefined HDX endpoint cannot be added to the Address Book on RMX with Avaya Call Manager. Second attempt yields message that participant name already exists in Address Book.	V7.0	
192	*Interoperability*	VNGR-16791	In a 1024Kbps conference with Auto layout, Sharpness, AES, H.239 Content to Legacy Endpoints and LPR enabled, Lifesize endpoints encounter poor video.	V7.0	

POLYCOM®

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
193	*Interoperability*	VNGR-16797	In H.323 and SIP calls to RMX with MPMx, Aethra X7 endpoint displays blurred, tiled video.	V7.0	
194	*Interoperability*	VNGR-16806	On RMX 1500, a macro block is displayed in the large video window of the video layout when PVX endpoint is the speaker.	V7.0	
195	*Interoperability*	VNGR-16810	On an RMX 1500 set to the Flexible mode and running an HD720p 2Mb conference with IVR, Gathering, High Profile, and Audio Clarity enabled, 15 PVX, HDX, VSX 300, 7000 CMAD endpoints cannot change layouts when DTMF codes are used.	V7.0	
196	*Interoperability*	VNGR-16820	VSX8000 endpoint connected to RMX 1500 with MPMx in 1920kbps conference, transmits green video to all endpoints but correctly displays all connected participants' video.	V7.0	
197	*Interoperability*	VNGR-16825	Using RMX 2000 with MPMx, H.320 call to VSX8000 endpoint fails with Call Disconnection Cause listed as "No net connection - 0 ".	V7.0	
198	*Interoperability*	VNGR-16841	Connect to the network using VPN and then start a conference with LPR enabled, connect endpoints using CMAD, the video of the endpoints was very fragmented.	V7.0	
199	*Interoperability*	VNGR-16856	Artifacts displayed on ISDN endpoints connected to RMX 1500 when content is started or stopped.	V7.0	
200	*Interoperability*	VNGR-16868	On RMX 1500 audio interruptions are experienced by CMAD endpoints.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
201	*Interoperability*	VNGR-16877	Avaya 1XC Softphone endpoints connected to conference on RMX do not receive content, while HDX endpoints do.	V7.0	
202	*Interoperability*	VNGR-16889	On RMX 1500 Video Preview - View Participant Received Video of VSX3000 endpoint is displayed as a green screen. Problem occurs at 384kbps, feature works correctly at higher call rates.	V7.0	
203	*Interoperability*	VNGR-16894	When the privacy shutter of a VVX1500 endpoint is closed, a mosaic is displayed instead of a black screen.	V7.0	
204	*Interoperability*	VNGR-16903	RMX 2000 with MPMx stops receiving calls from DMA. Subsequent calls disconnect with disconnection cause cited as Resources Deficiency.	V7.0	
205	*Interoperability*	VNGR-16921	On an RMX with version 7.0, when an Avaya 1XC Softphone dials Avaya 1XC Softphone when pressing the "Conference" button on the Avaya 1XC Softphone the Ad hoc conference on the RMX does not start.	V7.0	
206	*Interoperability*	VNGR-16924	In DMA, when a SIP endpoint is connected to a certain MCU, and the user chooses to stop using it, the call is routed to a different MCU while the call rate is reduced by 64k.	V7.0	
207	*Interoperability*	VNGR-16925	Avaya 1XC Softphone intermittently partially connects to conference RMX when connecting as 2nd or subsequent participant.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
208	*Interoperability*	VNGR-16938	Using Tandberg MXP endpoints, artifacts and choppy occur in video for 10 seconds after 1mbps H.323 or SIP connection to RMX 1500.	V7.0	
209	*Interoperability*	VNGR-16943	The Gathering slide turns green after changing layout on ViewStations when ViewStation SP Release 7.5.4.16 SP and ViewStation 512k Release 7.5.4.17 are connected to a conference running on RMX2000 with MPM+ at a Line Rate of 384Kbps, LPR, Same Layout and Auto Layout are enabled.	V7.0	
210	*Interoperability*	VNGR-16950	When RMX dials out from an encrypted conference running at 768Kbps, video quality set to Sharpness and with LPR enabled to H.323 HDX-A, the call connects OK. Then, H.323 HDX-B dials into HDX-A and the call connects OK. When HDX-B disconnects from HDX-A, the video freezes on HDX-A and RMX shows HDX-A as connected with problem.	V7.0	
211	*Interoperability*	VNGR-16955	iPower 9000 endpoint in H.323 call with RMX with MPM+ or MPMx does not transmit audio in encrypted calls.	V7.0	
212	*Interoperability*	VNGR-16960	Call on RMX 2000 with MPMx using HDX endpoint connects at 128Kbps with resolution HD720p even if RMX call rate is set for 8Mb.	V7.0	
213	*Interoperability*	VNGR-17073	Loss of lip sync occurs on HDX9004 endpoint talking to an HDX9000 endpoint in 2Mbps conference with the following mix of endpoints: H323, PSTN, PVX, CMAD, HDX, dialed in via DMA with LPR on, Gathering Off, Echo suppression on.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
214	*Interoperability*	VNGR-17221	Video from CMA-D participant was not displayed in call dialed via DMA to RMX4000 running V6.0.0.105 with 4*MPM+80 cards.	V6.0	
215	*Interoperability*	VNGR-17346	Striped video image of all other participants occurs on HDX8000 endpoint after dialing via DMA to RMX4000 running V7.0.1.16 with, 4*MPM+80 cards.	V7.0.1	
216	*Interoperability*	VNGR-17495	QDX6000 connects with a problem over H323 to a conference running on RMX 2000 with MPMx at a line rate of 192kbps or 128kbps, and LPR, Video Clarity and Send Content to Legacy Endpoints options enabled.	V7.0.2	
217	*Interoperability*	VNGR-17547	PVX H.323 endpoint cannot send content when connected to a conference running on RMX 2000 with MPMx, at a line rate of 384kbps.	V7.0.2	
218	*Interoperability*	VNGR-17559	Sony PCS-XG80 cannot connect to RMX 2000/1500 with MPMx over SIP.	V7.0.2	
219	*Interoperability*	VNGR-17589	RadVision Scopia XT1000 is connected with a problem to a conference running on RMX 2000 with MPMx at a line rate of 4MB and LPR and Encryption enabled after viewing the IVR Welcome slide.	V7.0.2	
220	*Interoperability*	VNGR-17606	LifeSize systems are sometimes locking up and disconnecting when connected to a CP conference running on RMX 4000 with MPM+ at a line rate of 1920kbps, video quality set to Sharpness and LPR, Video Clarity and Send Content To Legacy Endpoint options enabled.	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
221	*Interoperability*	VNGR-17636	VVX is displayed in two conference video layout cells when connected over H.323 to a conference that includes two VVX endpoints when the VVX comes off hold while in the gathering screen. One cell is live video and the other cell is frozen video.	V7.0.2	
222	*Interoperability*	VNGR-17652	After resuming the call that was placed on hold, VVX 1500 display does not return to Auto Layout and remains small in the top right corner of the display. The VVX is connected via H.323 to a conference running at 128Kbps.	V7.0.2	
223	*Interoperability*	VNGR-17668	Sony PCS-XG80 receives video at a resolution of 432x240 instead of 720p when connected to a CP conference running on RMX 2000 with MPM+ at a line rate of 1920kbps with LPR, Video Clarity and Send Content to Legacy Endpoint options enabled.	V7.0.2	
224	*Interoperability*	VNGR-17749	Flickering video is displayed for a few seconds on Lifesize Room 200 screen when connecting to a conference running on RMX 4000 at 4MB with Encryption and LPR enabled.	V7.0.2	
225	*Interoperability*	VNGR-17807	Radvison Scopia XT1000 does not transmit video when connected at a line rate of at 1920kbps to a CP conference running on RMX 2000 with MPMx and its Resource Configuration set for "Video Quality Optimized".	V7.0.2	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
226	*Interoperability*	VNGR-17823	No cropping, no border and shrunken video is displayed on the VVX endpoint when connecting a VVX endpoint, HDX endpoint and a Telepresence endpoint to a conference set to telepresence mode that is running on RMX 2000 with MPMx cards.	V7.0.2	
227	*Interoperability*	VNGR-3977	Faulty connection status is indicated when the RSS 2000 recording link is the only participant in a conference and its video stream is not synchronized.	V1.1.0	The video stream is synchronized when the first participant connects to the conference.
228	*Interoperability*	VNGR-4652	HDX/VSX endpoints cannot connect directly to conferences while registered with Cisco Gatekeeper using the IP##NID string.	V1.1.0	Connect directly using the MCU IP Address via the Transit Entry Queue.
229	*Interoperability*	VNGR-6902	Sony PCS G70 (v2.61) and Sony PCS-1(v3.41) endpoints cannot connect to conferences using SIP connections.	V5.1	Force the endpoints to connect using H.323 connection.
230	*Interoperability*	VNGR-7597	H.323 link is connected as secondary when cascading with Tandberg MPS at 768Kbps, in both Video Switching and CP conferences.	V3.0.0	
231	*Interoperability*	VNGR-7598	H.323 link is connected as secondary when cascading with Tandberg MPS at 768Kbps, in both Video Switching and CP conferences.	V3.0.0	
232	*Interoperability*	VNGR-8605	The video of Sony G70 endpoint that is connected to a conference over ISDN at line rate of 128Kbps freezes when receiving Content from an HDX endpoint.	V3.0.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
233	*Interoperability*	VNGR-9015	Radvision ECS Gatekeeper set to Routed Mode is not forwarding the LPR parameters as required, causing HDX calls with LPR enabled to connect with no video.	V3.0.0	
234	*Interoperability*	VNGR-9677	When switching Content sending from an HDX9004 to Aethra X7 and back, Content is not received by Aethra X7.	V4.0.0	
235	*Interoperability*	VNGR-9830	HDX endpoints may experience packet loss when the HDX endpoint's LAN Speed is configured to 100MB.	V4.0.0	Set the endpoint LAN Speed and Duplex Mode to Auto.
236	*Interoperability*	VNGR-9909	When dialing out to a Tandberg MXP ISDN endpoint, the IVR slide is not displayed, although the IVR message is played.	V4.0.0	
237	*Interoperability*	VNGR-20136	In an RMX 384Kb conference with a Cascaded MGC when H.323 and MPI participants connect to the conferences the cascaded link connects as Secondary.	7.5	
238	*IP*	VNGR-16617	When CMAD endpoint running on Lenovo R61connects to a Meeting Room whose Line rate is 1024 Kbps, Video quality is set to Motion, Content is set to HiRes Graphics and LPR, Same Layout and Echo Suppression options are enabled, after few minutes in the conference the CMAD observes packet loss in the People Rx although QoS is enabled.	V7.0	
239	*IP*	VNGR-7734	Static Routes table in IP Network Service does not function.	V3.0.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
240	*ISDN*	VNGR-12007	Occasionally, when ISDN participants connect to a conference with line rate 384kbs, multiple asserts appear in the log file.	V5.0.0	
241	*ISDN*	VNGR-12011	Occasionally, an ISDN participant fails to connect to the conference due to the following error - "MCU internal problem - 50020".	V5.0.0	
242	*ISDN*	VNGR-12034	In a conference running at a line rate of 384 Kbps, H.320 encrypted participant cannot connect and an assert appears.	V5.0.0	
243	*ISDN*	VNGR-15707	An RMX 4000 with a 384K H.320 conference with Motion and AES enabled, when a Tandberg 6000 MXP connects, the endpoint encounters video freezes.	V7.0	
244	*ISDN*	VNGR-16264	During a conference the ISDN line is functional but the line has no clock source.	V7.0	
245	*ISDN*	VNGR-16301	After starting a VSW conference with LPR enabled, when dialing out using ISDN a message appears: "SIP cannot connect to VSW with LPR enabled"	V7.0	
246	*ISDN*	VNGR-16726	On an RMX2000 with MPMx cards running an 383 Kbps ISDN conference when connecting 10 endpoints by blast dial-out the endpoints video showed black screens.	V7.0	
247	*ISDN*	VNGR-16863	On RMX 1500, ISDN endpoint is listed with "Connected With Problem" status.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
248	*ISDN*	VNGR-16879	In a 384Kbps H.320 conference with Video Clarity, Auto Terminate, Sharpness, Echo Suppression, Auto Layout, Gathering, and Send Content to Legacy Endpoints enabled, when the RMX dials-out to VS4000, FX, EX, VSX7000A and HDX9004 endpoints, flickering and video artifacts are seen.	V7.0	
249	*ISDN*	VNGR-16928	On RMX 1500, dial out from 256kbps conference to ISDN endpoint forced to 1920 kbps displays green screen and disconnects with "Internal MCU Problem".	V7.0	
250	*ISDN*	VNGR-16946	Video freezes on ISDN endpoints in a fully loaded RMX 2000 with MPMx when connecting, disconnecting and reconnecting all the endpoints at a line rate of 256Kbps.	V7.0	
251	*ISDN*	VNGR-16974	Blurred (Predator) video is displayed on the HDX endpoint that is in self view when a movement occurs while the endpoint is connected via ISDN to a conference running at a line rate of 1472kbps, with encryption enabled.	V7.0.2	
252	*ISDN*	VNGR-17574	Internal ISDN\PSTN Audio Only calls get a loud noise (static/pop) prior to the start of the IVR message.	V7.0.2	
253	*ISDN*	VNGR-17635	The video of ISDN participants freezes during a conference running at a line rate of 256kbps on RMX 2000 with MPMx and Encryption and LPR options enabled.	V7.0.2	Set the conference to a Line rate other than 256Kbps.

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
254	*ISDN*	VNGR-17645	Video artifacts (video stream is superimposed on the IVR Welcome slide) when an ISDN participant connects to a conference running on RMX 2000 with MPMx at a line rate of 384kbps.	V7.0.2	
255	*ISDN*	VNGR-17689	ISDN endpoints do not connect at line rates higher than 768kbps, irrespective of profile setting, whether dial-in or dial-out.	V7.0.2	
256	*ISDN*	VNGR-17887	Sometimes, HDX9006 2.7.0-5547 and VSX7000 9.0.6 endpoints connecting over ISDN to a conference running at 384kbps do not receive video.	V7.0.2	
257	*ISDN*	VNGR-4405	When a busy signal is returned by a PSTN dial-out participant, the RMX does not redial but disconnects the participant with "party hung-up-0" status.	V2.0.0	
258	*IVR*	VNGR-10054	Customized CIF slide is not displayed on the HDX screen when connecting to a 1080p High Definition Video Switching conference.	V4.0.1	
259	*IVR*	VNGR-11531	After upgrading the RMX to a software version that includes the gateway and the maximum number of IVR services reached 40 in RMX 2000 and 80 in RMX 4000, the default Gateway IVR Service is not created.	V4.1	
260	*IVR*	VNGR-12031	A conference running at a line rate of 1920Kbpsand IVR Service that includes a Welcome Slide, both the Welcome Slide and Video are partially blacked out.	V5.0.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
261	*IVR*	VNGR-12116	When a participant is moved from one conference to another and becomes the single participant in the destination conference, the participant does not hear music.	V5.0.0	
262	*IVR*	VNGR-15101	In a Video Switched 4Mbps conference, only the last part of DTMFs *6 (mute) and #6 (unmute) messages are heard.	V7.0	
263	*IVR*	VNGR-15131	In a conference started from a Profile, when an ISDN call is forced to Audio algorithm G722_1_C_24k a buzzing noise can be heard before the IVR starts.	V7.0	
264	*IVR*	VNGR-15831	When uploading a number of high and low resolution slides to an IVR service, there is only option to choose one slide.	V7.0	
265	*IVR*	VNGR-16313	On an RMX2000 with an MPMx card running a 512Kbps conference with Gathering, IVR, Echo Suppression enabled and resources set to a Flexible Mode, when dialing out using H.261 the IVR slide flashes.	V7.0	
266	*IVR*	VNGR-16460	On RMX 2000 with MPMx, H.261 endpoint that displays the default slide does not access nor displays a new slide that is added to the IVR Service.	V7.0	
267	*IVR*	VNGR-16539	In a mixed H.323 & SIP 128Kbps conference with Video Clarity, Sharpness, IVR Service and Welcome Slide settings set to "High profile optimized", when connecting HDX 8000 endpoints, the H.323 HDX endpoint does not view the IVR slide but a black screen for 15 seconds.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
268	*IVR*	VNGR-16556	In a mixed H.323 & SIP 128Kbps conference with Gathering, Sharpness and the Welcome Slide defined as "High Profile optimized", when connecting HDX8000 endpoints, the H.323 HDX video has artifacts on the Gathering slide.	V7.0	
269	*IVR*	VNGR-17615	iPower 9000 remains in the IVR Welcome stage when connecting to a CP conference running at 384kbps with Video Quality set to Motion and Video Clarity, Encryption, LPR and Send Content to Legacy Endpoint options enabled.	V7.0.2	
270	*IVR*	VNGR-17708	HDX8006 and HDX9006 remain in the IVR Welcome stage when connecting to a Video Switching conference running at 4MB with Video Quality set to Motion and video resolution set to 720p 60 fps.	V7.0.2	
271	*IVR*	VNGR-17833	RadVision Scopia XT1000 and Lifesize Room 200 remain in the IVR Welcome stage when connecting to a CP conference running at 4096kbps with Encryption and LPR enabled. Other endpoints connected normally.	V7.0.2	
272	*IVR*	VNGR-9834	When DTMF codes have been entered by the participants, the volume of the IVR Message may be suppressed or the message may be cut.	V4.0.0	
273	*LPR*	VNGR-10104	When an H.323 HDX endpoint sends Content, the endpoint disables the LPR.	V4.0.1	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
274	*LPR*	VNGR-16997	LPR is enabled by default in the conference profile when CP mode is selected. LPR is disabled by default in the conference profile when VSW mode is selected. Changing between CP and VSW modes causes LPR to be enabled/disabled.	V7.0	
275	*Multilingual*	VNGR-14332	The stop monitoring option (in right click on MCU) in the RMX manager is not translated to Japanese. VNGBE-851	V6.0	
276	*Multilingual*	VNGR-14333	Translation of the Exchange Integration Configuration dialog box is missing.	V6.0	
277	*Multilingual*	VNGR-14335	Several fields in the Conference Profile dialog box have not been translated.	V6.0	
278	*Multilingual*	VNGR-14336	Translations of some of the fields in the New Conference dialog box are missing.	V6.0	
279	*Multilingual*	VNGR-14338	Translation of the entries Copy Conference and past Conference in the Conference right-click menu is missing.	V6.0	
280	*Multilingual*	VNGR-14567	Translation of some of the fields in the Upgrade windows and dialog box are missing.	V6.0	
281	*Multilingual*	VNGR-14800	The translation of the Create Certificate button in the IP Network Service - SIP Server tab is missing.	V6.0	
282	*Multilingual*	VNGR-15812	Japanese translation is missing in some of the IVR Service dialog boxes.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
283	*Multilingual*	VNGR-16429	On RMX with Operator Conference selected in profile, when trying to delete a running conference, the popup message is displayed in mixed English and Japanese.	V7.0	
284	*Multilingual*	VNGR-5151	The Display Name of undefined dial-in participant using HDX and VSX 7000 endpoints is displayed in English in the RMX Web Client.	V2.0.0	
285	*Multilingual*	VNGR-5310	Multilingual Settings are not reflected on the Shelf Management login page and the multilingual flags appear in the Shelf Manager window even when they have not been selected in the Multilingual Settings pane.	V2.0.0	
286	*Partners - Microsoft*	VNGFE-3246	RMX disconnects MOC ICE Call between federated sites when RMX is not installed in the same site as the OCS Pool.	V7.0	Install the RMX on a main domain or federate the sub domain.
287	*Partners - Microsoft*	VNGR-13314	When resetting the RMX after loading the certificate and registering the RMX with the OCS, two active alarms appear: "SIP registration transport error" and "No response from Registration server".	V6.0	
288	*Partners - Microsoft*	VNGR-15798	In ICE environment, a green overlay is displayed on top of one of the video layout in the Gathering slide when a dial out MOC or HDX endpoint connect to the conference.	V7.0	
289	*Partners - Microsoft*	VNGR-17631	RMX does not identify the OC/4 version (Lync Server 2010/OCS-W14), hence the wrong video settings are used (4CIF instead of CIF).	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
290	*Partners - Microsoft*	VNGR-17743	In an environment that includes the Microsoft Lync server and RMX 4000 MPM+80 with ICE enabled, when the RMX dials out to two Lync clients with HDX connected, the second Lync client is disconnected from the conference that is running at 384kbps, with Encryption and LPR enabled due to a SIP HW internal MCU problem.	V7.0.2	
291	*Partners - Microsoft*	VNGR-17746	In an environment that includes the Microsoft Lync server and RMX 4000 MPM+80 with ICE enabled, when the Lync client escalates to video after connecting as Audio Only to a Meeting Room that is running at 384kbps, with Encryption and LPR enabled, artifacts appears at the start of the video.	V7.0.2	
292	*Partners - Microsoft*	VNGR-17753	In Microsoft Lync environment with ICE enabled, when the RMX 4000 with MPM+80 dials out to two Lync Clients (MOC1 with Creative Camera connected and MOC2 with CX5000 RoundTable connected), MOC1 does not receive video from MOC2.	V7.0.2	
293	*Partners - Microsoft*	VNGR-17757	In Microsoft Lync environment with ICE enabled, when a Lync client dials an Entry Queue running on RMX 4000 with MPM+80, the Lync client is not given enough time to enter the meeting room ID and is disconnect from the Entry Queue.	V7.0.2	
294	*PCM*	VNGR-15700	When PCM is initiated, site names are displayed over the PCM menu.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
295	*PCM*	VNGR-15757	Initiating PCM when there is only one endpoint connected to a conference that is receiving music results in the music being interrupted.	V7.0	
296	*PCM*	VNGR-15822	When PCM is activated in a Gathering-enabled conference, the PCM menu is displayed on top of the gathering slide instead of the display of the Gathering Slide being terminated before the PCM menu is displayed.	V7.0	
297	*PCM*	VNGR-16849	When H.263 participant uses PCM on RMX 2000 with MPM+, additional Video Windows appear in the Video Layout and the PCM menu appears with large letters on a blurred, colored display.	V7.0	
298	*PCM*	VNGR-16968	PCM is not supported with MPMx Cards.	V7.0	
299	*Recording*	VNGR-16947	In a conference running at 384Kbps and Gathering is enabled, recording is set to "Upon request" the recording is started once the gathering phase ends, resulting in the display of the Gathering slide and layout without text details and after 15 seconds the Gathering slide and layout remain and appear in the recording.	V7.0	
300	*RMX 1500 Audio*	VNGR-16857	On RMX 1500 metallic audio is heard periodically on PVX endpoint.	V7.0	
301	*Resource Capacity*	VNGR-19830	Changes to Voice Port allocation on RMX with two 2 IP Services defined requires a system reset to take effect. Voice participants cannot connect due to Resource Deficiency until reset is performed.	7.5	System reset.

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
302	*RMX 1500 General*	VNGR-16809	DTMF Code *71 (Secure Conference) sent to RMX 1500 displays Gathering Slide Text instead of "Secured" indicator text.	V7.0	
303	*RMX 1500 Video*	VNGR-16859	On RMX 1500 some endpoints display green flickering screen on layout change from 4x4 to 1x1.	V7.0	
304	*RMX 1500 Video*	VNGR-16867	On RMX 1500 with MPMx, when the endpoint displayed in the large video window in 2+8 layout disconnects, the large video window is not re-allocated to another endpoint.	V7.0	
305	*RMX 1500 Video*	VNGR-16901	On RMX 1500 Video Preview is preceded by a green screen momentarily before Video Preview starts.	V7.0	
306	*RMX 4000*	VNGR-14386	Display information for Slot 5, FSM (Fabric Switch Module), in the RMX 4000 Hardware Monitor is incomplete.	V5.1	
307	*RMX 4000*	VNGR-16892	On an RMX4000 with MPMx_D cards in the Hardware Monitor the RTM_LAN card is not listed.	V7.0	
308	*RMX 4000*	VNGR-17778	When trying to connect 180 V500/VSX to each of the two conferences running simultaneously on RMX 4000 with 4 MPMx-D cards, both conferences running at a line rate of 384, Video Quality set to Motion and Max CP resolution set to CIF, 180 participants connected to the first conference, while several participants out of the 180 could not connect to the second conference.	V7.0.2	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
309	*RMX Manager*	VNGR-14175	When using the RMX Manager, a Message Alert "500" is displayed when an RMX running Version 4.6 is selected in the MCU's list.	V6.0	
310	*RMX Manager*	VNGR-16677	Progress bar missing in RMX manager during upgrade.	V7.0	
311	*RMX Manager*	VNGR-17602	Double clicking on a card in Hardware monitor of the RMX Manager application displays the Card Properties dialog instead on the Processor Properties dialog box.	V7.0.2	
312	*RMX Manager*	VNGR-18170	Video Preview cannot be activated in RMX Manager application.	V7.0.2	
313	*RMX Manager*	VNGR-17861	RMX Manager fails to install from RMX Web Client login page.The request is aborted with the message: "Could not create SSL/TLS secure channel".	7.5	1. Install prior to initiating Secured Communications Mode 2. Install from a network. 3. Install locally from RMX Manager folder.
314	*RMX Manager*	VNGR-18414	Active Directory user cannot open the Hardware Monitor section in the RMX Manager.	7.5	
315	*RMX Web Client*	VNGR-12172	In the RMX Web Client, the main window opens up as full screen and cannot be resized.	V5.0.0	
316	*RMX Web Client*	VNGR-12257	When upgrading the RMX Web Client with software changes, Internet Explorer needs to be closed and opened before the upgrade can take place.	V5.0.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
317	*RMX Web Client*	VNGR-14778	ISDN/PSTN fields are disabled (grayed out) although Enable ISDN/ PSTN Dial-in check box is selected in RMX Management > Entry Queues > Default EQ.	V6.0	
318	*RMX Web Client*	VNGR-16210	On an RMX 1500 with a conference and connected participants, when multiple web clients are opened on different PC's and Video Preview is activated, when opening another browsing session and viewing Video Preview, all the browsers close though some view a "failure status" message.	V7.0	
319	*RMX Web Client*	VNGR-2473	Sometimes when installing the RMX Web Client, Windows Explorer >Internet Options> Security Settings must be set to Medium or less.	V1.1.0	
320	*RMX Web Client*	VNGR-7557	When connecting directly to the Shelf Manager and selecting Diagnostic Mode the CNTL module does not enter the diagnostic mode and stays "Normal".	V3.0.0	Reset the MCU and then switch to Diagnostic Mode.
321	*RMX Web Client*	VNGR-9829	Occasionally, during an ongoing conference, when selecting the Hardware Monitor menu the message "No connection with Switch" appears.	V4.0.0	
322	*Serial Gateway*	VNGR-20062	Only 108 out of 160 ports can connect to RMX4000 with MPM+80 cards. The next participant attempting connection is disconnected due to resource deficiency.	V7.5	
323	*SIP*	VNGR-11949	The maximum number of Meeting Rooms, Entry Queues, SIP Factories and ongoing conferences that can be registered to the Proxy, is limited to 100.	V5.0.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
324	*SIP*	VNGR-12006	With SIP defined and undefined dial-in participants you cannot change the layout type from "conference layout" to "personal layout".	V5.0.0	
325	*SIP*	VNGR-16535	SIP HDX sites (Version 2.6.1 and 2.6.0) receive video in resolution of 432x240 instead of 720p when connecting to a CP conference running on RMX 4000 at a line rate of 1920Kbps with 10+ layout selected and LPR is enabled.	V7.0	
326	*SIP*	VNGR-16663	In ICE environment, when connecting endpoints from all NAT environments (corporate/branch / enterprise) to an encrypted, 720p VSW conference, running at a line rate of 2M bps with video quality set to sharpness and video clarity and auto layout enabled, endpoints fail to connect to the conference with a disconnection cause "SIP request timed out".	V7.0	To overcome the problem do one of the following: * Connect the endpoints one by one. * Run a non encrypted 2M VSW conference * Run the conference at a lower line rate (768Kbps)
327	*SIP*	VNGR-16674	In ICE environment, when connecting endpoints from all NAT environments (corporate/branch/ federated) to an encrypted CP conference running at a line rate of 2Mbps, video quality set to sharpness, and video clarity and auto layout are enabled, some of the endpoints fail to connect due to TB_MSG_OPEN_PORT MCU internal problem or SIP HW MCU internal problem.	V7.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
328	SIP	VNGR-16839	On RMX with MPMx in High-Profile Motion conference at 512kbps, HDX endpoints connected via SIP only transmit H.264 HP / 4SIF at 15 frames per second.	V7.0	
329	SIP	VNGR-17562	The QDX6000 SIP endpoint is connected with problem to a conference running on RMX 4000 with MPM+ at a line rate of 768kbps and LPR, Video Clarity and Send Content To Legacy Endpoint options enabled.	V7.0.2	
330	SIP	VNGR-17626	SIP endpoint (no High Profile) connected at a resolution of SD30 instead of SD60 when connecting to a conference running on RMX 4000 with MPMx at a line rate of 1024kbps with LPR enabled and Video Quality set to Motion.	V7.0.2	Disable the LPR option.
331	SIP	VNGR-17627	High Profile enabled SIP endpoint connected at a resolution of SD30 instead of SD60 when connecting to a conference running on RMX 4000 with MPMx at a line rate of 512kbps with LPR enabled and Video Quality set to Motion.	V7.0.2	Disable the LPR option.
332	SIP	VNGR-17628	High Profile enabled SIP endpoint connected at a resolution of SD60 instead of 720p60 when connecting to a conference running on RMX 4000 with MPMx at a line rate of 1024kbps with LPR enabled and Video Quality set to Motion.	V7.0.2	Disable the LPR option.
333	SIP	VNGR-17633	Incorrect display name of the RMX is displayed on SIP endpoints. RMX Display name includes additional characters and not just the URI.	V7.0.2	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
334	*SIP*	VNGR-3276	SIP participants cannot connect to a conference when the conference name contains blank spaces.	V1.1.0	
335	*Software Version*	VNGR-8259	If an RMX operating in Secure Communication Mode, is downgraded to a version that does not support Secure Communication Mode (V2.0, V1.1), all connectivity to the RMX is lost.	V3.0.0	Cancel the Secure Mode before downgrading
336	*Software Version*	VNGR-19836	The Default IP Network Service configured using the Fast Configuration Wizard is not saved if no media cards are installed in the RMX during the configuration process.	7.5	
337	*Software Version*	VNGR-9228	When trying to restore last version, after upgrading from version 3 to version 4, the RMX prompts for an activation key.	V4.0.0	
338	*Software Version*	VNGR-20443	Active Alarm triggered by high CPU usage during RMX2000 startup.	7.5	
339	*Ultra Secure Mode*	VNGR-19998	MPM card becomes un-responsive after Card Software Recovery Procedure is performed while the RMX is in Ultra Secure Mode.		Remove and re-insert the MPM card while the system is running.
340	*Unified Communication Solution*	VNGR-13729	When connecting from a MOC endpoint using the link sent in the meeting invitation to an ongoing conference that was scheduled via the Polycom add-in for Microsoft Outlook on the RMX 4000 (standalone) with Gathering and Recording enabled, the conference is not started as a Meeting Room/Conference Reservation or ongoing conference with the same name already exist in the MCU.	V6.0	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
341	*Upgrade Process*	VNGR-12732	After upgrading the system from version 5.0 to version 4.6, the Users list is deleted and the default POLYCOM User is created. For security reasons, it is recommended to delete this User and create your own User.	V4.6	
342	*Upgrade Process*	VNGR-14720	After software Upgrade is completed, an Active Alarm "Connection to Exchange Server failed" appears in the Alarms List on the RMX4000.	V6.0	
343	*Upgrade Process*	VNGR-15904	When upgrading RMX4000 MPM+ from version 6.0.0.105 to version 7.0.0.91, the fault "Card voltage problem" is displayed for all installed cards.	V7.0	
344	*Upgrade Process*	VNGR-15907	When upgrading RMX4000 MPM+ from version 6.0.0.105 to version 7.0.0.91, the Fabric Switch name is missing from the Hardware Monitor.	V7.0	
345	*Upgrade Process*	VNGR-15909	When upgrading RMX4000 MPM+ from version 6.0.0.105 to version 7.0.0.91, the RMX Type (RMX4000) does not appear in the Hardware Monitor window.	V7.0	
346	*Upgrade Process*	VNGR-16258	Minor changes in the documentation to the upgrade process.	V7.0	
347	*Upgrade process*	VNGR-16422	RMX 2000 logs off during upgrade procedure when network is under stress.	V7.0	When the network is busy, use the RMX Manager application instead of the RMX Web Client to control the MCU.

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
348	*Upgrade Process*	VNGR-16462	When downgrading to software V6.0.0.105 and performing "Comprehensive restore" to Factory default, followed by upgrade to version V7.0.0.115 the upgrade procedure is stuck in "Software Loading" phase. System Reset (hard or soft) is required to resolve the problem.	V7.0	
349	*Upgrade Process*	VNGR-16752	On the RMX 2000/4000 with an ISDN card installed, after configuring the IP Fast Configuration Wizard, the system requests a reset and not to configure the ISDN Service.	V7.0	
350	*Upgrade Process*	VNGR-16817	After upgrading to version 7.0.0.135 the RMX Web Client shows that RMX is no longer in the "Startup" phase even though Faults list states: "Configuring".	V7.0	
351	*Upgrade Process*	VNGR-16886	On an RMX 1500/2000/4000 with MPMx cards, when upgrading to version 7.0 to build 139 and implementing the Diagnostic mode the MPMx card status remains in a "startup" phase.	V7.0	
352	*Upgrade Process*	VNGR-16954	On an RMX4000 after upgrading to version 7.0, build 148, the RMX "Could not complete MPM Card startup procedure".	V7.0	
353	*Upgrade Process*	VNGR-17411	Sometimes, the error message "Socket reconnected" is displayed after downgrading from V7.0.2.11 to V6.0.2.2.	V7.0.2	
354	*Upgrade Process*	VNGR-17768	When upgrading or downgrading the RMX 1500 software version and adding the activation key, the RMX Web Client disconnects from the RMX.	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
355	*Upgrade Process*	VNGR-18242	When upgrading RMX4000 with 4 MPM+ cards from Version 7.0.0.162 to Version 7.0.2.61 Two of the MPM+ cards remain in startup mode and do not complete the upgrade.	V7.0.2	
356	*Upgrade Process*	VNGR-18272	When downgrading an RMX 4000 with 4 MPMx cards from version 7.0.2.64 to version 7.0.1.16, the IMPC is burnt on only three out of four cards and the fourth card appears with voltage problem.	V7.0.2	
357	*Upgrade Process*	VNGR-18276	When upgrading an RMX 2000 with one MPM card from version 7.0.1.16 to version 7.0.2.64, the MPM card appears to be in normal state in the Hardware Monitor but with no available units. The status LED on the card is green as in normal status. The upgrade procedure takes longer to complete, and until it does the audio controller units cannot be used.	V7.0.2	
358	*Upgrade Process*	VNGR-18278	No access to RMX 2000 after software upgrade from version 7.0.2.61 to version 7.0.2.64.	V7.0.2	
359	*Upgrade Process*	VNGR-9565	When downgrading from version 4.0 to version 3.0, the MPM card does revert to normal.	V4.0.0	
360	*Upgrade Process*	VNGR-9740	When upgrading from version 2.0.2 to version 4.1, and then Restoring the Factory Defaults, during system restart sometimes MPL failure is encountered.	V4.0.0	Turn the MCU off and then turn it on ("hardware" reset)."

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
361	*Upgrade Process, Video*	VNGR-16215	Create conference set to High Profile and connect Durango endpoints, the Durango and HDX8000 Video preview is in a green color.	V7.0	
362	*Video*	VNGR-10239	In a 4Mb conference set to Sharpness and the IVR Welcome Message enable video appears in a 4x3 format. Disable IVR Welcome message and the video appears in 6x9 format.	V4.0.1	
363	*Video*	VNGR-11351	When the video from an endpoint is blocked, inconsistent video resolution settings are implemented.	V4.1	
364	*Video*	VNGR-11382	Legacy endpoints receive Content in 1+7 layout with black stripes on the sides (for aspect ratio fitting), selecting a different layout using Click&View (**) causes the black stripes to disappear.	V4.1	
365	*Video*	VNGR-11843	In a 2 Mb Video Switched conference with 10 or more H.323 endpoints connected, random video refreshes may occur.	V5.0.0	
366	*Video*	VNGR-11965	In a conference running at a line rate of 384 Kbps, with AES and LPR enabled, calls connect using the H.263 instead of the H.264 video protocol.	V5.0.0	
367	*Video*	VNGR-13001	Video display freezes momentarily with every speaker or layout change in a conference with HDX and SVX endpoints.	V4.6	
368	*Video*	VNGR-13152	Message overlay is limited to 32 Chinese characters OR 96 ASCII characters.	V4.6	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
369	*Video*	VNGR-14124	On rare occasions in 2Mbps ISDN calls, ISDN participants connected without their endpoints sending video for a few seconds.	V6.0	
370	*Video*	VNGR-15155	In a conference with a line rate of 4096kbps, set to Sharpness, 1+5 layout, after connecting a few endpoints, when an endpoint dials out, video In & Out freeze.	V7.0	
371	*Video*	VNGR-15386	Artifacts present in the Gathering Slide in 2560kbps, CP conference with Motion selected.	V7.0	
372	*Video*	VNGR-15495	Connect to a conference with HDX 8000 & 9000 endpoints, FECC on some of the endpoints starts only after 10 seconds.	V7.0	
373	*Video*	VNGR-15541	Create a conference on the RMX using the default factory video profile, connect a Sony PCS-G50 endpoint, and then try to control the XG80's camera. There is no response.	V7.0	
374	*Video*	VNGR-15709	In a 2MB CP conference with LPR, Gathering, Sharpness, Video Clarity and Auto Brightness enabled, when connecting SIP & H.323 PVX/HDX endpoints, when starting PCM and selecting 1*1 Layout, the conference video has video artifacts.	V7.0	
375	*Video*	VNGR-15722	On an RMX 4000 with MPM+ cards, when trying to view the Video Preview window, video is occasionally absent.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
376	*Video*	VNGR-15724	On RMX with MPMx, when a skin without background is selected, the Polycom skin background is displayed. When a skin with a background is selected, the speaker notation color is incorrect.	V7.0	
377	*Video*	VNGR-15738	When monitoring a conference and right-clicking a participant, the participant's video and audio freezes.	V7.0	
378	*Video*	VNGR-15763	A conference started from a Profile set to "Motion" and Video Resolution "HD 1080" after connecting HDX endpoints, resources used are incorrect.	V7.0	
379	*Video*	VNGR-16050	When using the MPMx card to run a conference with Auto Brightness enabled, no difference can be seen in the video between a light and darkened room.	V7.0	
380	*Video*	VNGR-16245	The resolution 1080p60fps is not available on the RMX 1500/2000/4000	V7.0	
381	*Video*	VNGR-16337	On an RMX 4000 in a 4096Kbps conference with Auto Terminate, Sharpness, Encryption, LPR, Echo Suppression, Auto Layout enabled, when dialing out to 40 HDX endpoints video corruption occurred.	V7.0	
382	*Video*	VNGR-16384	On an RMX 2000 with the MPMx card with a conference running, when HDX endpoints connect, sometimes in some of the video cells the Aspect ratio is incorrect when the source is 4:3 - and destination is 16:9.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
383	*Video*	VNGR-16618	On an RMX with MPM+ cards, when configuring the resolution of Configuration Slider to HD 1080p60/ HD 720p60 - in the participant properties you should not be able to select HD1080/HD 720p as the Maximum Resolution (People Video Definition).	V7.0	
384	*Video*	VNGR-16657	In a 4MB HD1080p conference with Content, Video Clarity, Auto Termination, Encryption, LPR, Echo Suppression and Auto Layout enabled, when dialing out to six HDX8006 endpoints and changing the speaker, all endpoints had bad video.	V7.0	
385	*Video*	VNGR-16695	Using MPMx, frame rate in motion conference is less than 60fps on HDX endpoints that connect at HD resolution at 1920kbps and are not allocated on the Turbo DSP.	V7.0	
386	*Video*	VNGR-16708	The displayed resolution of the gathering slide differs between H.323 participant (432x240) and H.320 participant (480x352) when both endpoints are connected to a CP conference running at a line rate of 384Kbps with video quality set to Motion and LPR is enabled. Once the Gathering phase ends, all participants connect with 2SIF resolution.	V7.0	
387	*Video*	VNGR-16722	On RMX 2000 with one MPM-H, small artifacts are displayed in the Gathering Slide when the configuration is changed to Presentation Mode during the Gathering Phase.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
388	*Video*	VNGR-16724	On RMX 1500, video display freezes momentarily during Video Layout changes before the new Video Layout is displayed.	V7.0	
389	*Video*	VNGR-16725	Blinking video occurs during ISDN blast dial-out at 384kbps on RMX 2000 with MPMx.	V7.0	
390	*Video*	VNGR-16782	On an RMX 1500, when adding 45 VSX and V500 endpoints to a 348 Kbps CIF CP conference, with Motion, Echo Suppression and Auto Layout enabled, VSX8000 endpoints connect using incorrect resolutions and video stills are encountered.	V7.0	
391	*Video*	VNGR-16796	On RMX with MPMx, Intra request from endpoint connected via H.264 CIF stream can sometimes take almost 1 second to be answered.	V7.0	
392	*Video*	VNGR-16812	When connecting 15 PVX, HDX, VSX 3000/ 7000 CMAD endpoints to a 2Mb HD720p conference with IVR, Gathering, High Profiles and Audio Clarity enabled, running on an RMX 1500, changing the conference layout from 1x1 to 4x4 (10+) results in brief video freezes.	V7.0	
393	*Video*	VNGR-16858	When connecting to 10 HDXs to a 4096Kbps conference with Encryption, LPR, Auto Termination, Sharpness, Auto Brightness, Audio Clarity and a 1x1 conference Layout enabled, running on an RMX2000 with MPM+ cards, the Welcome screen on one of the endpoints is partially fuzzy.	V7.0	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
394	*Video*	VNGR-16880	When connecting HDX & VSX endpoints to a mixed ISDN & IP 4096Kbps conference with Auto Terminate, Encryption, LPR, Sharpness, Auto Layout, Same Layout and Video Clarity enabled, running on an RMX 2000 with MPM+ cards, and muting and unmuting them, HDX endpoints encounter flickering video.	V7.0	
395	*Video*	VNGR-16944	Conferences running at a line rate of 768 and 1024Kbps with Gathering enabled may display distorted font and discolored background at 432x240, 512x288, 848x480 and 720x400 resolutions.	V7.0	
396	*Video*	VNGR-16952	During a 1472Kbps conference with LPR, AES, Gathering, Send Content to Legacy Endpoint and Auto Layout enabled, the video of VSX7000 and HDX8006 endpoints does not appear in the conference layout.	V7.0	
397	*Video*	VNGR-16958	During a 128Kbps conference with AES, Gathering, Motion, Send Content to Legacy Endpoints and Auto Layout enabled, empty layout cells, poor video and video stills occur in HDX, VSX, Lifesize endpoints.	V7.0	
398	*Video*	VNGR-17139	In a DMA 2Mb dial-in conference with LPR enabled and 20 mixed endpoints (HDX, VSX, CMAD H323, PSTN), three DSP video failures occurred and frozen video was viewed on two HDXs.	V7.0	
399	*Video*	VNGR-17148	Participant is seen blurred when connecting with QVGA resolution to a conference layout of 1+7.	V7.0.1	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
400	*Video*	VNGR-17156	In a DMA dial-in Meeting Room with several endpoints, a few endpoints viewed Zebra video artifacts.	V7.0	
401	*Video*	VNGR-17208	Video in layout 1+7 from VSX3000 is not displayed in conference with endpoints that dialed via DMA to RMX4000 running V7.0.0.162 with 4*MPM+80 cards.	V7.0	
402	*Video*	VNGR-17215	In a Dial-in Meeting Room with mixed (HDX8000/9004) endpoints, the endpoints viewed zebra video.	V7.0.1	
403	*Video*	VNGR-17220	documentation: Horizontal black lines are displayed across the video window on all endpoints in calls dialed via DMA to RMX4000 running V6.0.0.105 with, 4*MPM+80 cards.	V6.0	
404	*Video*	VNGR-17272	In a DMA Dial-in Meeting Room with several endpoints, HDX9004 viewed distorted video from other endpoints	V7.0.1	
405	*Video*	VNGR-17282	In a DMA Dial-in Meeting Room with several HDX8000 endpoints, video transmission stopped.	V7.0.1	
406	*Video*	VNGR-17291	In a Dial-in Meeting Room, endpoints viewed impaired video and occasionally received bad audio.	V7.0.1	
407	*Video*	VNGR-17302	Black screen with normal audio occurs on HDX8002 endpoint that dialed via DMA to RMX2000 running V7.0.1.16 with 2*MPMX cards.	V7.0.1	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
408	*Video*	VNGR-17363	Endpoint connects at a higher resolution than expected according to the Resolution Slider configuration when line rate of the endpoint is forced to a lower rate than the conference rate. For example, if the conference line rate is 1024kbps and the endpoint line rate is forced to 512kbps, the endpoint resolution upon connection will be 720p instead of SD (as if it was connected at 1024Kbps).	V7.0.2	
409	*Video*	VNGR-17377	High Profile enabled HDX 8000 remains in the Gathering layout with frozen video inside the cells after blast dial out to several endpoints of type HDX 8000/ HDX 9004 / HDX 4000/ VSX 8000/ VSX 3000 from a CP conference at a line rate of 512kbps and LPR enabled.	V7.0.2	
410	*Video*	VNGR-17379	Green video image occurs on HDX8000 v2.6.0-4740 endpoint after dialing to RMX 2000 running V7.0.1.16 with, 2*MPM+80 cards.	V7.0.1	
411	*Video*	VNGR-17484	Periodic video freezes on H.323 endpoints when connected to a CP conference running on RMX 1500 at a line rate of 4096kbps and AES and LPR options enabled.	V7.0.2	
412	*Video*	VNGR-17514	An empty cell is displayed in the video layout when muting and then unmuting individual endpoints that are connected to the conference as follows: 10 ISDN at a line rate of 128kbps, 7 HDX 8006 at a line rate of 4096kbps, 15 HDX 9004at a line rate of 1024kbps and 15 VSX 384kbps.	V7.0.2	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
413	*Video*	VNGR-17525	A black vertical line is displayed between cells where usually there is a border when OTX and RPX 400 endpoints are connected to a conference running on RMX system with MPMx at a line rate of 4MB and video Quality set to Sharpness.	V7.0.2	
414	*Video*	VNGR-17539	Objects in video sent from VSXs are displayed stretched horizontally on HDXs screens when all are connected to a conference running on RMX 1500 over H323 and SIP.	V7.0.2	
415	*Video*	VNGR-17542	VSX8000 sees frozen video of the Gathering slide when connected over H.323 or ISDN to a conference running on RMX 1500 at a line rate of 1024kbps and LPR, encryption and Send Content to Legacy Endpoint options enabled.	V7.0.2	
416	*Video*	VNGR-17571	Rainbow bar appears when changing the conference layout from CP_LAYOUT_1X2 or from CP_LAYOUT_1X2HOR to CP_LAYOUT_1X2VER or CP_LAYOUT_2X1 in a conference running on RMX 2000 with MPMx, at a line rate of 4096kbps, Video Quality set to SHARPNESS and Video Clarity, Encryption, LPR and Echo Suppression options enabled.	V7.0.2	
417	*Video*	VNGR-17580	Site names are blinking when connecting H.261/263 participants to the conference.	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
418	*Video*	VNGR-17611	Video seen on HDX8006/7006 screen looks superimposed and blotchy after changing the video layout to full screen when connected via H.323 to a conference running on RMX 2000 with MPMx at a line rate of 384kbps and Encryption and LPR options enabled.	V7.0.2	
419	*Video*	VNGR-17640	Video freeze occur when connecting the 74th HD 720p participants (out of 80) to a conference running on RMX 4000 with 4 MPM+80 cards at a line rate of 1MB, Video Quality set to Sharpness and Video Clarity, encryption and LPR options enabled.	V7.0.2	
420	*Video*	VNGR-17644	Video freeze occur when connecting 40 HD 720p participants to a conference running on RMX 2000 with 2 MPM+80 cards at a line rate of 1MB, Video Quality set to Sharpness and Video Clarity, encryption and LPR options enabled.	V7.0.2	
421	*Video*	VNGR-17646	H.261 participant video is not seen by other conference participants and the Gathering text did not appear on the H.261 participant's screen when connected to a conference running at 512kbps. The H.261 participants sees the conference video correctly.	V7.0.2	
422	*Video*	VNGR-17657	The VVX takes over a minute to resume live video on other endpoints in conference after releasing the hold when connected over H.323 to a conference running on RMX 1500 at a line rate of 128kbps.	V7.0.2	

Table 8 *Version 7.0.2 System Limitations*

#	Category	Key	Description	Detected in Version	Workaround
423	*Video*	VNGR-17679	Video freeze occur when connecting 20 HD 1080p participants to a conference running on RMX 2000 with 2 MPM+80 cards at a line rate of 4MB.	V7.0.2	
424	*Video*	VNGR-17742	Poor video quality due to low frame rate is viewed on HDX systems when connecting to a CP conference running on RMX 2000 with MPMx at a line rate of 6MB, with LPR, Video Clarity and Gathering options enabled.	V7.0.2	
425	*Video*	VNGR-17796	A thin gray line is present at the bottom of the cells when connecting TPX and RPX endpoints to a conference running on RMX 2000/4000 with MPMx cards at a line rate of 3MB or higher and video quality is set to sharpness.	V7.0.2	
426	*Video*	VNGR-17841	Lip sync occurred when an endpoint connected at 512kbps to a conference running at line rate of 2MB on RMX 2000 with 2 MPM+80 cards, and LPR enabled and active due to packet loss.	V7.0.2	
427	*Video*	VNGR-17857	Sometimes the Gathering text is not displayed when connecting SIP and H.323 endpoints to a conference running on RMX 2000 with MPMx at a line rate of 1920kbps.	V7.0.2	
428	*Video*	VNGR-17888	Full screen layout is displayed instead of 3x3 layout when the 3x3 layout is selected using Click&View from HDX9004 version 2.7.0-5547. Conference is running on RMX 2000 with either MPM+ or MPMx.	V7.0.2	

Table 8 Version 7.0.2 System Limitations

#	Category	Key	Description	Detected in Version	Workaround
429	*Video*	VNGR-18106	Empty cells are displayed in the video layout when connecting 30 HDX 8006 endpoints at a line rate of 4MB and resolution of 1080p to a conference running on RMX 2000 with 2 MPMx-D cards.	V7.0.2	
430	*Video*	VNGR-18279	The video display is "jumpy" when endpoints connect to a conference running on RMX with MPMx at a line rate of 512Kbps and SD resolution.	V7.0.2	